UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, v. KEITH RANIERE, Defendant.	Case No. 1:18-cr-00204-NGG-VMS **NON-STATUTORY MOTION TO COMPEL POST-JUDGMENT MATERIAL & EXCULPATORY DISCOVERY** **EVIDENTIARY HEARING REQUESTED** **ORAL ARGUMENT REQUESTED**

SUMMARY

While Mr. Raniere has awaited the Court's Order on his Motion for a New Trial Pursuant to Rule 33, in anticipation of an evidentiary hearing and possibly a new trial, he has retained four new digital forensic experts, in addition to the three experts who submitted affidavits in the initial Rule 33 Motion. Of these now seven experts, four are former FBI employees. (Ex. A-1 to A-8.) Engagement with these experts has made clear that a short list of narrowly tailored exculpatory evidence possessed by the government must be provided to Mr. Raniere and his legal team to comport with constitutional due process requirements. While discovery issues were raised in the Rule 33 Motion based on a broader list of evidentiary items, Mr. Raniere now respectfully submits this non-statutory motion to compel discovery so that the Court may order the government to disclose this narrowly tailored list of evidentiary items to the Defense, pursuant to the legal principles of fundamental fairness discussed herein, as well as the interests of judicial economy.

FACTS

As best described in Mr. Raniere's Motion for New Trial, *United States v. Raniere*,18-cr-204-1 (NGG) (VMS) Dkt. 1169, his original trial was fatally flawed by the admission of falsified evidence. Specifically, digitally manipulated images were manufactured and/or altered and planted on a camera card and hard drive to make it appear as if Mr. Raniere photographed twenty-two nude pictures of a fifteen-year-old and then retained them on a computer hard drive. Presently, the government refuses to provide Mr. Raniere with each of the four evidentiary items requested below, which it has in its possession and could easily disclose with minimal effort and expense. The evidence at issue, *which has never been provided to Mr. Raniere*, would allow his experts to further substantiate the evidence of manipulation in his underlying criminal case, proving his innocence to the allegations, and thereby necessitating a new trial.

Having received the reports of Dr. J. Richard Kiper, in a letter dated March 16, 2022, Mr. Raniere's undersigned counsel requested from the government eighteen evidentiary items relevant to the evidence manipulation that occurred in Mr. Raniere's underlying criminal case. (Ex. B.) In a letter dated March 16, 2022, the government refused to provide any additional discovery. (Ex. C.) However, each of the four evidentiary items requested herein is essential to further investigate the evidence manipulation, with the strong likelihood of discovering more instances of manipulation and precisely when it occurred and who performed it. (Ex. D & E.)

The evidence requested falls into three categories: (1) two forensic copies of a camera card and corresponding FTK log files; (2) a file listing from the hard drive, which was alleged to have contained the contraband images; and (3) CART examination notes.

1. Camera Card

Mr. Raniere requested and should be provided with copies of the two camera cards:

- A forensic copy of the CF card dated April 11, 2019, NYC024299.001, and the corresponding FTK log file, NYC024299.001.txt

- A forensic copy of the CF card dated June 11, 2019, NYC024299_1B15a.E01, and the corresponding FTK log file, NYC024299.1B15a.E01.txt

These evidentiary items would allow the experts to examine the content and metadata of the 37 new files that appeared on the June 11, 2019, FTK report that were not present on the April 11, 2019, FTK Report, to find additional proof of manipulation, and possibly determine how and when some of the manipulation was done, including what tools were used. (Ex. D & E.)

2. File Listing of the Hard Drive

By reviewing the hard drive's file index list, Defense experts can determine whether the manipulation present on the hard drive occurred before or after the government imaged it. (Ex. D & E.) Accordingly, Mr. Raniere should be provided with:

- The CSV file listing for the image of the WD hard disc drive taken on September 19, 2018 (NYC023721_1B16.E01.csv).

3. **CART Examination Notes and FTK Log Files**

Examination notes were presumably taken by CART Examiner SFE Flatley when he inspected the camera card for the Canon camera. These notes, and the corresponding FTK log files, are integral to determining whether the 37 new files were added after SFE Flatley analyzed the camera card or had existed beforehand. (Ex. D & E.) Accordingly, Mr. Raniere should be provided with SFE Flatley's examination notes for the camera and camera card, Evidence Item Number 1B15,[1] and the FTK log files associated with his examination.

Mr. Raniere requested these evidentiary items as soon as it became apparent that they would assist in establishing his innocence and proving that the child pornography evidence was

[1] *United States v. Raniere*,18-cr-204-1 (NGG) (VMS) Government Trial Exhibit hereafter "GX 520 & 524."

fabricated. These evidentiary items are exculpatory, given that it has now been conclusively proven that the evidence used against Mr. Raniere at trial was extensively altered and manipulated and, damningly, that each instance of alteration and manipulation supported the government's trial narrative. These four requested items will reveal further information about when and how the evidence used against Mr. Raniere at trial was manipulated. (Ex. D & E.)

The FBI, too, should have a clear interest in understanding how, when, and why evidence in its custody was tampered with and by which agents –not only to vindicate Mr. Raniere's civil rights, but to protect itself from future incidences of illegal misconduct and attendant appeals.

Therefore, the government's refusal to disclose these items forces Mr. Raniere to bring this supplemental motion now, requesting an order for the disclosure of these four pieces of exculpatory evidence forthwith.

ANALYSIS

There is no legitimate argument to deny Mr. Raniere access to the evidence that will demonstrate the method and extent of the manipulation done by government witnesses to the two key pieces of digital evidence at the heart of the government's case against Mr. Raniere. Since this discovery will lead to further expert findings on how the contraband images were manufactured by being given false dates, it will reflexively prove Mr. Raniere's innocence on these key allegations. Accordingly, Mr. Raniere now brings this motion respectfully requesting that this Court compel the government to disclose said discovery, as such is mandated by the due process principles discussed herein.

I. Due Process Requires That the Government Disclose the Requested Evidence to Mr. Raniere Upon the Court Granting Him a New Trial Under Rule 33.

Under *Brady*, the prosecution violates a defendant's right to due process if it withholds

evidence that is favorable to the defense and material to the defendant's guilt or punishment. *Smith v. Cain*, 565 U.S. 73, 75 (2012).

"[E]vidence is 'material' within the meaning of *Brady* when there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different." *Id*. citing *Cone v. Bell*, 556 U.S. 449, 469–470 (2009). A reasonable probability does not mean that the defendant ***"would more likely than not have received a different verdict with the evidence," only that the likelihood of a different result is great enough to "undermine confidence in the outcome of the trial."*** *Cain, supra,* 565 U.S. at 75-76, citing *Kyles v. Whitley*, 514 U.S. 419, 434 (1995) [emphasis added].

Here, under the current circumstances, this Court should grant Mr. Raniere's Rule 33 Motion for a New Trial. Consequently, the government will be required to disclose the requested evidence because, as described herein, it is exculpatory and is therefore subject to mandatory disclosure under *Brady*[2] and its progeny.

The government's failure to provide either NYC024299.001, the forensic copy of the camera card, which FSE Flatley analyzed on April 11, 2019, or NYC024299_1B15a.E01, the forensic copy of the camera card, which FSE Booth analyzed on June 11, 2019, prevented Mr. Raniere's trial team's the ability to timely discover the evidence manipulation and the ability to present the proof of such during trial. Had the government timely disclosed the requested evidence to the Defense, the Defense would have shown the camera card to be incompetent evidence, leading to its exclusion from trial. Notwithstanding its exclusion, being able to prove that the camera card bore the unmistakable markings of manipulation by government witnesses would have hurt the government's case and aided Mr. Raniere in presenting a defense.

[2] *Brady v. Maryland*, 373 U.S. 83 (1963).

Consequently, there is a reasonable probability that, had the evidence at issue been disclosed to Mr. Raniere, the result of his trial would have been different. Thus, the failure to disclose the forensic copies of these camera cards in the prejudgment phase of Mr. Raniere's case was, inescapably, violative of *Brady*.

Accordingly, there is no reason to delay the inevitable; the government must disclose this exculpatory evidence.

II. Regardless of the Post-Conviction Status of this Case, Mr. Raniere has Due Process Rights to the Requested Evidence Items.

"[W]here the government holds previously produced forensic evidence, the testing of which concededly could prove beyond any doubt that the defendant did not commit the crime for which he was convicted, the very same principle of elemental fairness that dictates pre-trial production of all potentially exculpatory evidence dictates post-trial production of this infinitely narrower category of evidence. And it does so out of recognition of the same systemic interests in fairness and ultimate truth." *Dist. Attorney's Office for the Third Judicial Dist. v. Osborne*, 557 U.S. 52, 95-98 (2009); citing *Harvey v. Horan*, 285 F.3d 298, 317 (4th Cir. 2002.)

In fact, this Court has opined that "[T]he fact that a prosecutor's *Brady* disclosure obligation ends at judgment does not insulate prosecutors from accountability for earlier, prejudgment *Brady* violations. ***A post-conviction movant or habeas petitioner may obtain post-judgment relief for these prejudgment Brady violations***." *Wright v. U. PO, Parole Officer*, 10-CV-5127 (MKB) *36, fn.32 (E.D.N.Y. Jul. 2, 2021) [emphasis added].

"[I]t would simply be 'constitutionally intolerable,' for the government to withhold from the convicted, *for no reason at all,* the very evidence that it used to deprive him of his liberty, where he persists in his absolute innocence and further tests of the evidence could, given the circumstances of the crime and the evidence marshaled against the defendant at trial, establish to

a certainty whether he actually is factually innocent of the crime for which he was convicted. *Harvey v. Horan* (4th Cir. 2002) 285 F.3d 298, 318 [internal citations omitted, emphasis in original].

In *Osborne*, the issue before our Nation's High Court was whether to allow the Defense access to biological evidence items to test using STR technology, "with which it is ***often possible*** to determine whether a biological tissue matches a suspect with ***near certainty***." *Osborne, supra,* at 557 U.S. 52, 62 [emphasis added].

Here, while DNA disclosure commonly has a statutory basis and did have such in *Osborne*, in the case at hand, there is a stronger argument for disclosing digital evidence under a non-statutory, procedural due process basis than the disclosure ordered in *Osborne*. Unlike DNA, digital evidence is non-exhaustible; a copy can be made without impacting the original evidence or the government's possession thereof. While disclosure would not hamper further testing by the government on the original items, it would allow a fair opportunity for the Defense to test the copied items. Because digital evidence is not biological, both shipping and storage are easier than with biological samples, which were ordered disclosed in *Osborne*. Moreover, while the STR technology at issue in *Osborne* "is extremely discriminating," *Osborne*, supra, 557 U.S. at 60 fn.3, STR technology, and DNA testing in general, always leaves some remaining doubt; the results are not absolute and instead are based on percentages and ratios. On the other hand, digital forensics results are absolute as they provide ***mathematically certain*** results.

Just as in *Osborne*, the government here possesses the four previously produced evidentiary items at issue. Because each of these items can be subjected to scientific testing

related to investigating a crime, they are forensic evidence.[3] Further, the testing of these items will prove beyond any doubt that Mr. Raniere did not commit Racketeering Acts 2 and 3, sexual exploitation of a child, or Racketeering Act 4, possession of child pornography, all three of which were found to be "proved" by the jury. *However, if the twenty-two photos were, in fact, contraband, there would be no reason for anyone to tamper with the metadata to make them appear to be contraband*. It is indisputable that seven forensic experts have found that each instance of alteration of the digital evidence, in this case, appears to have been done to support the government's trial narrative. (Ex. A1-A8, *United States v. Raniere*,18-cr-204-1 (NGG) (VMS) Dkt. 1169 at Ex. D, E, & F.) In fact, based on the opinion of seven different forensic experts who reviewed the currently available evidence, further testing would not only prove Mr. Raniere's innocence as to these allegations, but it would also demonstrate that bad actors in the government tampered with the evidence to obtain a false conviction. Thus, the Court should order the disclosure of the four evidentiary items requested.

Further, according to this Court's opinion in *Wright*, although Mr. Raniere's case is in post-conviction status, he may obtain post-judgment relief for the government's earlier, prejudgment suppression of the evidentiary items at issue as such suppression constituted *Brady* violations. As discussed in previous filings, forensic data shows that evidence manipulation was done to key evidentiary items, the camera card, and the hard drive. Evidence related to this manipulation would therefore be material. Moreover, since this requested evidence helps to further prove the manipulation, its introduction in court would have hurt the government's case and helped Mr. Raniere's defense on the issue of the child pornography evidence, which was the

[3] Forensic, *Cambridge Dictionary, Cambridge University Press & Assessment* (2023) found at https://dictionary.cambridge.org/us/dictionary/english/forensic.

basis of the predicate acts of possession of child pornography and sexual exploitation, of which the government stated was "at the heart" of their racketeering conspiracy. *United States v. Raniere* 18-cr-204-1 (NGG) (VMS) Status Conference Transcript (March 18, 2019) at 19:8-16. Thus, these items are the very definition of *Brady* material. See *Smith v. Cain* (2012) 565 U.S. 73, 75. Therefore, the government committed Brady violations because these items were not disclosed before or during trial. Consequently, in line with this Court's opinion in *Wright*, the government is not insulated from these earlier prejudgment *Brady* violations. Therefore, this Court should afford Mr. Raniere Mr. post-judgment relief by ordering the government to disclose the four requested evidentiary items.

Additionally, the *Horan* Court's measure of constitutional intolerability would undoubtedly apply in the instant case. There is *no reason at all* for the government here to continue to withhold from Mr. Raniere these four evidentiary items which were used to convict him of the most heinous allegations against him, where, not only does he persists in his absolute innocence, but such innocence is bolstered by reputable forensic experts who have affirmed that further testing of the four requested evidentiary items could, given the circumstances of the crimes and the evidence marshaled against Mr. Raniere at trial, establish to a certainty that he actually is factually innocent of the crimes for which he was convicted. (Ex. D & E.)

Notably, *by the government's own admission*, disproving the child pornography and sexual exploitation allegations - racketeering acts 2, 3, and 4 - would go far towards proving Mr. Raniere's actual innocence of Count One - racketeering conspiracy - as in their own words, "[T]he child pornography is also at the heart of our racketeering conspiracy." *Raniere*, *supra*,18-cr-204-1 (NGG) (VMS) Status Conference Transcript (March 18, 2019) at 19:8-16.

Not only was the racketeering conspiracy the foundation of the government's case against Mr. Raniere; without it, the government did not have jurisdiction over any of its allegations against Mr. Raniere. Because these four items will bolster and expand the experts' previous findings regarding the manipulation of the alleged child pornography, these items will hit at the very heart of the government's case against Mr. Raniere and thus are relevant and material to proving his actual innocence.

While there were eleven racketeering acts alleged, and a conviction under RICO only requires that two of the acts be found, the jury had to enter findings as to each act, so there is no question in the verdict that the jury found acts two, three, and four – those related to possession of child pornography and sexual exploitation of a child – to be "proved." *Raniere, supra,*18-cr-204-1 (NGG) (VMS)Trial Tr. at 5747:5-15. However, those three racketeering acts comprise the two most heinous accusations an individual can face and the only alleged conduct involving a minor in this case. It is irrefutable that including these three racketeering acts in a second superseding indictment *on the eve of trial* pervaded every facet of Mr. Raniere's trial on a fundamental level from that point forward. Proof of this is that when these three heinous racketeering acts were charged, all other co-accused immediately requested severances and/or accepted plea bargains. *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) at Dkt. 1169 at 7-9. Importantly, the notions of procedural due process and fundamental fairness do not distinguish between wrongful criminal accusations based on whether they are counts or racketeering acts; if someone is factually innocent of what the government accuses them of and there is readily available evidence that can prove such, then procedural due process and fundamental fairness demand disclosure of such evidence. See *Osborne*, *supra*, 557 U.S. at 95-98.

Moreover, the importance of proving that government witnesses conspired to manufacture and plant child pornography on a hard drive and then link it to Mr. Raniere cannot be overstated. As the seven submitted expert affidavits have shown, Mr. Raniere was deprived of fundamental Constitutional rights due to this manipulation. *Mathews v. Eldridge,* 424 U.S. 319, 332 (1976) [Procedural due process imposes constraints on governmental decisions which deprive individuals of "liberty" or "property" interests within the meaning of the Due Process Clause of the Fifth or Fourteenth Amendment].

Further, Mr. Raniere was deprived of the ability to adequately confront his accusers - the government's FBI witnesses - about their relation to the evidence manipulation. He was also deprived of the ability to present experts to show that the only two pieces of digital evidence used to prove the most heinous of the allegations against him, the camera card and the hard drive, were not only incompetent but also manufactured through government malfeasance. *See California v. Trombetta* 467 U.S. 479, 486 fn. 6 (1984).

Such heinous violations of fundamental Constitutional rights would upend the entirety of Mr. Raniere's case and necessitate a new trial, if not an outright dismissal of all charges. Further, the government's case at a retrial would be severely hampered by the disqualification of the twenty-two alleged contraband photos, the camera card where the twenty-two photos were alleged to have originated, and the Western Digital hard disc drive where they were alleged to have been stored. This is not to mention the difficulty of proffering testimony from FBI agents who either refuse to testify by invoking their Fifth Amendment rights or who bear convictions for involvement in a criminal conspiracy to tamper with the specific evidence at issue in this case.

The government intentionally suppressed the four evidentiary items at issue by not disclosing them to the Defense before and during trial. Further, despite reasonable requests by the Defense, the government continues to intentionally suppress said evidence. The evidence at issue is dispositive to the current and continuous due process violations against Mr. Raniere in that said evidence is expected to vindicate him for the crimes for which he was convicted. *Horan, supra,* 285 F.3d at 318. Such a calculus remains unaltered despite the post-conviction status of this case. *Osborne, supra,* 557 U.S. at 95. Accordingly, due process and fundamental fairness necessitate governmental disclosure of the evidentiary items. *Id*.

Seven independent experts, including four former FBI examiners, have analyzed the evidence that has been available to the Defense, and all seven have concluded that there are definitive demarcations of manipulation and falsification of evidence, with the most logical explanation being government bad actors. (Exhibit A1-A8; *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Dkt. 1169 at Ex. D, E, & F.) It is a reasonable conclusion that these four items contain further evidence of manipulation, which is exculpatory to Mr. Raniere, and will directly disprove major portions of the government's case against him.

Because there has been conclusive proof of alteration and manipulation of critical evidence in this case, by government witnesses, it is paramount that the government disclose the four requested evidentiary items to the Defense. The initial bringing to light of the malfeasance in this case occurred nearly a year ago, on May 3, 2022, in the filing of the Motion for a New Trial Pursuant to Rule 33. Since then, much time has passed to give the opportunity for possible further manipulation.

CONCLUSION

For the above reasons, Mr. Raniere respectfully requests the Court to order the government to disclose the requested evidence.

Dated: April 14, 2023,

Respectfully submitted,

/s/ Joseph M. Tully_____
Joseph M. Tully*
Martinez, CA
CA SBN 201187
Tully & Weiss Attorneys at Law
713 Main Street Martinez, CA 94553
Phone: (925) 229-9700
Fax: (925) 231-7754
Admitted pro hac vice

Attorney for Defendant Keith Raniere

EXHIBIT A-1

CURRICULUM VITAE

Stacy R Eldridge, CFCE, GCFE, LPD

Digital Forensics Expert, Cybersecurity Expert, and Expert Witness
145 Hackberry St, Bennet NE 68317
Phone: 402-413-1517 | Email: stacy@siliconprairiecyber.com

EDUCATION

2006 **Master of Science** – Computer Information Systems
Bellevue University, Bellevue, NE

2001 **Bachelor of Science** – Management Information Systems
Bellevue University, Bellevue, NE

PROFESSIONAL EXPERIENCE

2021 – Present **Adjunct Professor**
Bellevue University
Teaches cybersecurity and digital forensics courses. Evaluates students' performance.

2020 – Present **Adjunct Professor**
Oklahoma State University Institute of Technology
Teaches cybersecurity and digital forensics courses. Evaluates students' performance.

2019 – Present **Founder, Digital Forensics and Cybersecurity Expert**
Silicon Prairie Cyber Services LLC
Provides cybersecurity awareness and simulated phishing consulting and program management services. Conducts digital forensics investigation and review services, including expert witness testimony. Licensed Private Detective in the State of Nebraska; fully bonded and complying with all statutes, rules, and regulations to conduct digital investigation services and provide expert witness testimony in a court of law. Licensed Plain Clothes Detective authorized to work at the direction of other detective agencies.

2017 – 2019 **Director, Cyber Security**
Lincoln Electric System (LES)
Leads and matures the information technology (IT) and operational technology (OT) cybersecurity strategy, risk mitigation, risk tolerance, risk assessment programs, and written policy. Developed tactical and strategic plans to ensure the continued development of cybersecurity maturity and protection of IT and OT networks and critical infrastructure, including sensitive LES information.

2012 – 2017 **Senior Staff Cyber Investigator & Program Manager, Data Loss Prevention**
General Electric
Conducted 1,030 DLP investigations and identified 236 violations that resulted in further escalation and investigation. Managed global, operational program protecting GE's crown jewels, critical business information, intellectual property, and sensitive data by implementing new and innovative technologies to simplify and accelerate manual processes to block, review, identify, and remediate unauthorized data egress. This program supports Corporate, Digital, GGO, and GO.

2003 – 2012 **Federal Bureau of Investigation Experience**

Digital Evidence Instructor
Operational Technology Division
Provide digital forensics, and investigative training focused on preserving, acquiring, examining, and presenting digital evidence. Develops curriculum, manuals, and presentations and selects subject matter expert guest lecturers. Designs, develops, and modifies materials presented in digital forensics and investigative training courses. Create test data sets, written tests, and hands-on practical forensic examination tests and grading requirements. Maintain liaison with professional law enforcement organizations, federal agencies, academic institutions, the computer industry, and private companies involved in investigative, digital evidence, and computer technology matters. Prepares and maintains classroom facility consisting of three separate networks, servers, and workstations.

Computer Analysis Response Team Forensic Examiner
Operational Technology Division
Los Angeles Division
Columbia Division
Omaha Division
As a computer forensic examiner for the Los Angeles Division, forensically examines computers and computer-related digital media, adhering to documented standard operating procedures and quality assurance programs, which includes annual proficiency testing; technical, peer, and administrative reviews.

Conducts forensic examinations on digital evidence (computers, computer-related digital media, cell phones, smartphones, personal digital assistants (PDAs), and digital cameras. Provides written and electronic reports summarizing examination results, provides advanced analysis of examination results as requested, and performs search and seizure operations to preview and acquire evidence on site.

Conducts research and career development activities, completes required continuing education, advanced specialized training, and yearly proficiency testing. Provide instruction to new examiners, peers, and federal, state, and local investigators.

Provides expert witness court testimony.

Information Technology Specialist
Omaha Division
Coordinates the daily operations of applications that function independently or as an integrated system. This included both stand-alone computers and local area networking. Resolved complex processing issues and error conditions requiring intricate processing software changes and served as the office authority concerning the capabilities and potential of online applications and individual computer programs used to support administrative and investigative efforts. Duties also included installing, configuring, and maintaining the FBI Omaha Intranet server, Internet server and router, and Internet local area network.

CERTIFICATIONS & AWARDS

Licensed Private Detective
FBI Certified Computer Analysis Response Senior Team Forensic Examiner (CART SFE)
FBI Certified Computer Analysis Response Team Forensic Examiner (CART FE)
FBI Certified PDA Forensic Examiner
FBI Certified Cell Phone Forensic Examiner
IACIS Certified Forensic Computer Examiner (CFCE)
GIAC Certified Forensic Examiner (GCFE)
AccessData Certified Examiner (ACE)
GIAC Security Essentials (GSEC) Certification

Network+ Certification - CompTIA
A+ Certification - CompTIA
2011 Outstanding Performance as a CART Examiner Award
2008 CART Gold Quality Award
Three FBI Performance Awards
FBI Quality Step Crease (QSI)
2013 General Electric Expertise Aware

EXPERT WITNESS – DIGITAL FORENSICS

2007	United States District Court for the District of South Carolina, Charleston, SC
2009	United States District Court for the Middle District of Florida, Tampa, FL
2011	United States District Court for the Central District of California, West Covina, CA

PROFESSIONAL TRAINING

Aug 2022	SANS 2022 Security Awareness Summit
Aug 2022	SANS 2022 DFIR Summit
Oct 2021	Nebraska Cybersecurity Conference
Aug 2021	SANS 2021 Security Awareness Summit
Aug 2021	SANS 2021 DFIR Summit
Oct 2020	Nebraska Cybersecurity Conference
Aug 2020	SANS 2020 Security Awareness Summit
Aug 2020	SANS 2020 DFIR Summit
July 2020	Cyber Threats in the Time of COVID-19 (Infragard)
May 2020	Taking a byte out of Chromebook Analysis
May 2020	Magnet Virtual Summit
Nov 2019	GRIDEX V
Oct 2019	SANS Windows Forensic Analysis
Feb 2019	FTK Intermediate
April 2018	SANS Implementing and Auditing the Critical Security Controls - In-Depth
March 2018	2018 Optiv Enterprise Security Solutions Summit
Feb 2018	DHS Intermediate Cybersecurity for Industrial Control Systems (202)
Feb 2018	DHS Intermediate Cybersecurity for Industrial Control Systems (201)
Feb 2018	DHS Introduction to Control Systems Cybersecurity (101)
Nov 2017	GRIDEX IV
Oct 2017	SANS Security Essentials: Network, Endpoint, and Cloud
Sept 2017	MRO 2017 Technical Training
Sept 2017	MRO 2017 Security Conference
May 2017	SEI CERT Insider Threat Symposium
May 2017	Enfuse Conference by Guidance Software
May 2016	IACIS Windows Forensic Examiner Training
May 2015	IACIS Macintosh Forensic Examiner Training
Dec 2014	EnCase Host Intrusion Methodology and Investigations
May 2014	IACIS Windows Forensic Essentials
Oct 2013	Cyber Security Summit
Sept 2013	SEI CERT Insider Threat Workshop
June 2013	Lean Six Sigma Quality
May 2013	Encase 101 v.7
March 2013	Searching and Reporting with Splunk
July 2012	NW3C Basic Data Recovery & Analysis (BDRA)
Oct 2011	EnCase Mac and Linux
July 2011	FTK Lab Advanced Train the Trainer (FBI)
July 2011	FTK for Mac (FBI)
May 2011	Sumari Mac Forensics (FBI)
March 2011	Encase Advanced Internet Exams (FBI)

Jan 2011	Encase II
Dec 2010	Encase I
Dec 2018	Proficiency Grading Workshop (FBI)
Sept 2010	Proctored Moot Court (FBI)
Sept 2010	Senior Moot Court (FBI)
Aug 2010	Advanced Forensic Analysis (FBI)
July 2010	Linux Command Line (FBI)
April 2010	IACIS Advanced Internet Investigations
May 2010	IACIS Advanced Certified Examiner Training
March 2010	Virtual Forensics (FBI)
Oct 2010	Digital Camera Forensics (FBI)
Aug 2009	Certified Ethical Hacker Training
Aug 2009	RCFL Phone Forensics Course (FBI)
May 2009	XRY Cell Phone Forensics (FBI)
March 2009	EnCase Computer Forensics II
Nov 2008	ImageScan 3 Training (FBI)
Sept 2008	Linux for LEOs (FBI)
June 2008	Microsoft Vista (FBI)
Feb 2008	AccessData Vista & Advanced Topics (FBI)
Dec 2007	eDiscovery Training (Infragard)
Aug 2007	Introduction to Internet Investigations
July 2007	Cell Phone Forensics (FBI)
June 2007	Security+ FBI)
June 2007	RCFL Webinar (FBI)
April 2007	Proctored FTK Boot Camp (FBI)
Mar. 2007	AccessData Applied Decryption (FBI)
Jan. 2007	Search Concepts - Self-paced Workbook (FBI)
Nov. 2006	Proficiency Test Grading Workshop (FBI)
Nov. 2006	Proctored CART Practicals (FBI)
Oct. 2006	Instructor Development Course (FBI)
Sept. 2006	Image Scan Training (FBI)
Sept. 2006	Case Agent Investigative Review Training (FBI)
Aug. 2006	Linux Boot CD v5 for FEs (FBI)
July 2006	AccessData Internet Forensics (FBI)
June 2006	PDA Forensics (FBI)
June 2006	NW3C Intermediate Data Recovery and Analysis (IDRA)
May 2006	CART Coordinator Workshop (FBI)
May 2006	FBI Anti-Piracy/Protection of Intellectual Property Rights Seminar
Apr. 2006	Microsoft Advanced Forensics (FBI)
Mar. 2006	Introduction to Cyber Crime (FBI)
Jan. 2006	AccessData FTK (Advanced) (FBI)
Dec. 2005	Proficiency Test Grading Workshop (FBI)
June 2005	Internet Processing (FBI)
Aug. 2005	CART Moot Court (FBI)
May 2005	CART Practicals (FBI)
May 2005	FTK Boot camp (FBI)
Mar 2005	Network+ (FBI)
Mar. 2005	NW3C Basic Data Recovery & Analysis (BDRA) (FBI)
Feb. 2005	BWCT Forensic Concepts Self-Paced (FBI)
Jan. 2005	A+ (FBI)
Dec. 2004	BWCT Write Protection & Imaging Self-Paced (FBI)
Dec. 2004	BWCT Quality Management (FBI)

EXHIBIT A-2

Affidavit of Stacy R Eldridge

State of Nebraska
County of Lancaster

COMES NOW Stacy R Eldridge, being first duly sworn, under oath, and states that the contents of the following attached reports, including their appendices, and exhibits are true and correct statements of relevant facts and his opinions in the case of United States v. Keith Raniere et. al., in the United States District Court, Eastern District of New York, Case #: 1:180-cr-00204-NGG-VMS, to the best of his knowledge and belief:

- Summary of Technical Findings dated 9/29/2022
- Summary of Process Findings dated 9/29/2022

Signature: Stacy R Eldridge

Address: 1145 Hackberry St
Bennet, NE 68317

SUBSCRIBED AND SWORN TO before me this 29th day of September, 2022, by Stacy R Eldridge.

Debra A. Grant
NOTARY PUBLIC FOR NEBRASKA

GENERAL NOTARY - State of Nebraska
DEBRA A. GRANT
My Comm. Exp. February 8, 2023

My Commission Expires: 02/08/2023

Stacy R. Eldridge, CFCE, GCFE, LPD
FBI Senior Forensic Examiner (Former)
Digital Forensics and Cybersecurity Expert

September 29, 2022

Summary of Technical Findings

Background

I worked as an employee of the FBI from 2003 to 2012. During that time, I served as an Information Technology Specialist (ITS), a Forensic Examiner (FE) on the Computer Analysis Response Team (CART), a Senior Forensic Examiner (SFE) on CART, and a Digital Evidence Instructor for CART Headquarters.

Within those roles, I conducted over four hundred examinations on over 100 TBs of data, mentored and trained CART Forensic Examiners in Training (FETs), trained and graded Special Agents in the Digital Evidence Extraction Technician (DeXT) program, trained and graded CART FETs on Quality Manuals, Standard Operating Procedures, and evidence processing, and graded CART FE yearly proficiency tests, and trained law enforcement personnel to use Image Scan.

After serving in the FBI, I worked as a Senior Staff Cyber Investigator and Program Manager at General Electric, and Director of Cybersecurity at Lincoln Electric System. I currently provide cybersecurity and digital investigation services.

Review of Evidence

My review and analysis of information included: AccessData Forensic Tool Kit (FTK) Reports and file directory listings produced by the Government of 1B15 (a Lexar CF Card) and 1B16 (a Western Digital Hard Drive), SFE Booth's CART examination notes, drag and drop copy of 1B16 that excluded alleged contraband, a file directory listing of 1B16, court testimony, government exhibits, defense exhibits, government discovery items, search warrants and associated affidavits, chains of custody for 1B15 and 1B16, rule 33 submission submitted by the defense, and reports and portions of work product generated by Dr. J. Richard Kiper as provided to me.

I have examined the data used by Dr. J. Richard Kiper discussed in his "Summary of Technical Findings Report," issued on April 25, 2022. Based on my examination, I agree with the facts as stated in his findings below.

1. Some digital photo files found on the CF card had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people. Moreover, these same CF card files contained thumbnail pictures from another existing set of photos, thus proving manual alteration of the CF Card contents.
2. Additional files appeared on the FBI's forensic report of the CF Card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the CF Card and the WD HDD.
3. An unknown person accessed the CF card on 9/19/18, thereby altering file system dates, while it was in the custody of FBI Special Agent Michael Lever.

4. Dates of photos on the hard drive were altered through manual intervention. The alterations seem to be an attempt to account for Daylight Saving Time.
5. The metadata of a modified photo, whose numbered filename appears between the alleged contraband ranges, was manually altered to create the appearance that it had not been modified.
6. The folders containing the alleged contraband and others that supported the dating of the photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.
7. The photos in this case, including the alleged contraband photos, appear to be on the hard drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates.

Summary of Findings

The data on the compact flash card (1B15(b)) was altered and manipulated while in the custody of SA Lever of the FBI, who, as a case agent, is not authorized to review this evidence directly. The second FBI examination of the CF Card included additional files not present in the first examination, and some of those files were clearly falsified. Such as four photos matched their alleged backed-up copies on the hard drive by name and modified dates. However, the photos depict a different person in a different location than their counterparts on the hard drive. This would mean that the same camera had to have taken pictures of two different people in two different locations at the same exact time, which is impossible. The most plausible explanation is that a combination of photos and information was added to the CF Card and then manually manipulated to strengthen the relationship between the CF Card and hard drive, and the narrative that all of the photos in question on the hard drive were taken in 2005.

Without a doubt, files, folders, dates, and metadata on the hard drive (1B16) were manipulated. The photos in this case, including the alleged contraband, were planted on the hard drive and appear as if they are part of a backup. Furthermore, several subfolders named after dates/times used the wrong time and point to a human naming the folders after modified dates while forgetting to use a 24-hour clock instead of a 12-hour clock to include the ones containing the alleged contraband. The Government used no other data on the hard drive to establish the validity of the dates of the photos other than information that is easily altered and was indeed deliberately altered, as evident by the remnants of human error left behind. Presently, there is no way to scientifically pinpoint when these alterations on the hard drive were made, but they align with the Government's narrative that the photos were taken in 2005. Moreover, these manipulations appear to be part of an elaborate attempt to manufacture a timeline to support photos taken in 2005, but ultimately a trail of mistakes was left behind.

In this case, it is my expert opinion that the digital evidence was extensively manipulated, and some of this manipulation, specifically regarding the CF card, was executed by a person or persons within the FBI.

Sincerely,

Stacy R Eldridge

Stacy R. Eldridge, CFCE, GCFE, LPD

Stacy R. Eldridge, CFCE, GCFE, LPD
FBI Senior Forensic Examiner (Former)
Digital Forensics and Cybersecurity Expert

September 29, 2022

Summary of Process Findings

Background

I worked as an employee of the FBI from 2003 to 2012. During that time, I served as an Information Technology Specialist (ITS), a Forensic Examiner (FE) on the Computer Analysis Response Team (CART), a Senior Forensic Examiner (SFE) on CART, and a Digital Evidence Instructor for CART Headquarters.

Within those roles, I conducted over four hundred examinations on over 100 TBs of data, mentored and trained CART Forensic Examiners in Training (FETs), trained and graded Special Agents in the Digital Evidence Extraction Technician (DeXT) program, trained and graded CART FETs on Quality Manuals, Standard Operating Procedures, and evidence processing, and graded CART FE yearly proficiency tests, and trained law enforcement personnel to use Image Scan.

After serving in the FBI, I worked as a Senior Staff Cyber Investigator and Program Manager at General Electric, and Director of Cybersecurity at Lincoln Electric System. I currently provide cybersecurity and digital investigation services.

Review of Evidence

My review and analysis of information included: AccessData Forensic Tool Kit (FTK) Reports and file directory listings produced by the Government of 1B15 (a Lexar CF Card) and 1B16 (a Western Digital Hard Drive), SFE Booth's CART examination notes, drag and drop copy of 1B16 that excluded alleged contraband, a file directory listing of 1B16, court testimony, government exhibits, defense exhibits, Government discovery items, search warrants and associated affidavits, chains of custody for 1B15 and 1B16, rule 33 submission submitted by the defense, and reports and portions of work product generated by Dr. J. Richard Kiper as provided to me.

I have examined the data used by Dr. J. Richard Kiper discussed in his "Summary of Process Findings Report," issued on April 25, 2022. Based on my examination, I agree with the facts as stated in his findings below. I also discovered an additional violation of FBI policy (see V and VI below).

- Receiving unsealed evidence created a broken Chain of Custody.
- The CF Card was accessed by an unauthorized FBI employee.
- The timeline of examination is suspicious.
- Critical evidence was withheld from the defense team.

Summary of Findings

Never in my ten years in the FBI have I seen so many violations of critical FBI policies and procedures applied to key evidence, all in one case, where the CART team included not one but two senior forensic examiners. The fact that these policy violations occurred to digital evidence that, according to my technical analysis, was manipulated while in FBI custody is suspicious and troubling.

Thus, it is my expert opinion if the defense and the Court had been aware of these policy violations, in combination with findings of data manipulation, I do not believe this digital evidence would have been allowed in as evidence during the trial.

I. Unsealed Evidence is Not Normal

The FBI has a policy that applies to all FBI personnel that dictates how digital evidence is to be handled, preserved, and examined. First, all digital evidence is to be secured and sealed to prevent loss, damage, and harm; this ultimately protects the integrity of the device and its data. When the integrity of evidence is not protected, any information gleaned from it could be called into question because anything could have happened to it while it was unsealed. A chain of custody is used in conjunction with this policy to protect the integrity of evidence and document who was responsible and accountable for its protection during that period.

During my time in the FBI, I was trained that digital evidence must always be received sealed, and if it was not, then it should be documented in exam notes, and I trained CART personnel the same. I cannot recall a time in over four hundred exams in the FBI when I received unsealed evidence for routine examination. In this case, the Government downplayed the severity of the fact that the CF Card was not sealed when it was given to CART for examination in June of 2019, nor was it documented in the exam notes.

II. Unauthorized and Prohibited Review of Original Digital Evidence

The same FBI policy also dictates who can review original digital evidence and in what order. Original digital evidence is to be given to CART personnel for examination first, and only after that can other personnel review a copy (not the original). This case is especially troubling because at least two persons in the FBI, SA Maegan Rees and SA Michael Lever, conducted unauthorized and prohibited reviews of the CF Card before the evidence was given to CART, as documented on the Chain of Custody. Even more troubling, I found evidence that the data on the CF Card was altered while in possession of SA Lever. Not only did unauthorized personnel review original digital evidence, but they also did so without a write blocker. They did not protect the integrity of the data. And in fact, they altered some of the data on it. Any time digital evidence is reviewed, it must be documented. I have not received any reports written by SA Rees and SA Lever documenting their unauthorized reviews of original digital evidence.

III. Untimely Examination of the CF Card

All of the evidence in the case except for 1B15 was submitted to CART for examination on 8/18/2018. Even though SA Rees and SA Lever had reviewed 1B15 in July and September of 2018, the CF Card was not submitted to CART until 2/22/2019. 2/22/2019 happened to be the same day a new search warrant was issued authorizing the search for child pornography on the hard drive only. Since SA Rees and SA Lever reviewed the contents of 1B15 five months earlier, one can logically assume the CF Card was identified at that time and should have been submitted to CART just like the rest of the digital evidence. I have trouble identifying an innocent explanation for this breach of protocol. Thus, I am left with the questions: Why didn't either Special Agent submit the CF Card to CART sooner? Did their unauthorized reviews not find any evidence pertaining to the search warrant?

IV. Unauthorized and Prohibited Re-Examination of Original Digital Evidence

The FBI policy only allows one examination of original digital evidence. Based on the FTK Report, the first FBI exam of the CF Card was completed on 4/11/2019 by SFE Stephen Flatley. An unauthorized re-examination of the CF Card was started at the tail end of the trial on 6/10/2019, as documented in SFE Brian Booth's exam notes. SFE Booth documented that the process to gain approval for a re-examination was not followed. Furthermore, there was no need for a re-examination because SFE Booth could have obtained access to the case on the CART Storage Area Network, a backed-up copy of the case from evidence control, or asked SFE Flatley for his working copy. After SFE Flatley completed the first exam, he provided the CF Card to SA Elliot McGinnis, who held it over the weekend, and then provided it to SA Christopher Mills, who had it for approximately seven hours and finally provided it to SFE Booth. It took four days to get the CF Card from one CART examiner to another who presumably worked in the same physical location. SFE Booth completed his re-examination on 6/11/19 with wildly different results. I have difficulty seeing an innocent explanation for this when taken together with the CF Card changing hands three times in four days before arriving in an unsealed bag to SFE Booth. I am left without an innocent answer based on the information provided to the defense for the following question: How could two highly trained Senior Forensic Examiners in CART have such drastically different results?

CART Examiners are allowed to analyze the processed evidence repeatedly. Any additional analysis only requires additional notes and reporting. This is a frequent occurrence during an investigation and trial preparation. While in the FBI, I conducted additional analysis numerous times without imaging and processing the evidence again. On occasion, when the first CART Examiner is unavailable, another CART Examiner can review the CART notes, CART reports, and open the FTK case to conduct additional analysis. The evidence doesn't need to be imaged or processed again. Thus, one must ask, why did SFE Booth process the evidence again when it was not required? FBI policy specifically prohibits re-examination to protect the integrity of the evidence. In this instance, it seems that integrity was again not protected, as evidenced by four photos on the CF Card that matched their alleged backed-up copies on the hard drive by name and modified dates. However, the photos depict a different person in a different location than their counterparts on the hard drive. The most plausible explanation I can deduce is that the violations in FBI evidence-handling policy resulted in the alteration of the evidence.

V. Providing Original Digital Evidence to the US Attorney's Office is Prohibited

Per FBI policy, only an image or working copy of original digital evidence may be provided to the USAO. In this case, I found evidence of the CF Card, original digital evidence, being provided to the USAO. On 9/27/2018, AUSA Tanya Hajjar told the Court, "I think one of those was like 8 Hale camera, for example. We just pulled out the pictures out and gave them [the defense] everything." The 8 Hale camera she is referring to is 1B15. How was the USAO able to pull everything off of the CF Card? One can only conclude they were given the original digital evidence to do this since CART had not been given this piece of evidence yet.

The Government's letter regarding discovery is dated 9/25/2018 and describes the photos pulled off from 1B15 as VDM_NXIVM00005028-VDM_NXIVM00005130. These items were provided to the defense in two PDF files. Both of these PDF files were created on 9/21/2018 and authored by TCarby. It's logical to assume that TCarby is Terri Carby, a paralegal specialist in the USAO, as documented in a press release dated 7/12/2022 regarding the Attorney General's awards.

Again, these files were created nearly five months before the CF Card was provided to CART for examination. It is unknown how TCarby obtained the files to include in discovery, but the chain of custody for the CF Card indicates SA Lever had custody of the CF Card on the date TCarby created the PDF files.

In my ten years of experience at the FBI, I am unaware of a single case where the USAO office handled digital evidence before the FBI. I'm left with the question, why did the USAO's office handle the CF Card in September 2018 when it was only an 'accidental' discovery five months later that demonstrated the significance of this piece of evidence?

VI. Unauthorized and Prohibited Examination by an Outside Agency

A forensic tool was used to produce the photos included as items VDM_NXIVM00005028-VDM_NXIVM00005130 (as noted above), including deleted and carved files. A forensic tool must be used to recover deleted and carved files; this process is considered an examination in the FBI. This is significant because not only is it against FBI policy, the FBI did not conduct the first examination of the CF Card. It is unknown who conducted the examination, their training, what procedures were followed to create these results, or what steps were taken to protect the CF Card's integrity.

It's also important to note that these files provided by the Government as part of the discovery visually appeared to match only the results of the FTK Report dated 4/11/2019 and not the 6/11/2019 FTK Report. This further calls into question the reliability of the information present on the CF Card on 6/10/2019 and causes one to wonder what was done to the CF Card between the first and second FBI examinations.

VII. The Unreliability of EXIF Data

In this case, EXIF data from the CF card and the hard drive played a central role in the Government's narrative used to convict, and SFE Flatley and SFE Booth examined the CF card. In the past, SFE Flatley has testified on EXIF data's reliability. In a different trial, SFE Flatley

testified EXIF data was easily altered and unreliable. In this trial, SFE Booth testified to the opposite and that EXIF data was difficult to alter and highly reliable. In my experience, personally and professionally, it is my expert opinion that EXIF is easily modified by a person knowledgeable in computers without special software, and EXIF data by itself is unreliable.

VIII. Critical Evidence was withheld from the defense team

The defense was not provided with an image (a forensic copy) of the CF Card created by SFE Flatley or by SFE Booth. Nor were they provided any logs and file directory listings that accompany the images. The FTK processing logs from the exams conducted by SFE Flatley or SFE Booth were not provided. Only the PDF version of the FTK Report created by SFE Booth was provided, not the report's HTML version. This is significant because some hyperlinked files were not included in the PDF version of the report. I have not received any of these items either. Without these critical pieces of information, the defense and the jury were not provided with all of the information in this matter.

Conclusion

Based on my FBI experience and knowledge of FBI policies and procedures, it is my expert opinion that personnel in the FBI violated several critical FBI policies, procedures, and best practices when handling digital evidence.

Sincerely,

Stacy R. Eldridge, CFCE, GCFE, LPD

EXHIBIT A-3

Mark Bowling

33 Sosegado Lane, Hot Springs Village, AR 71909 | m.d.bowling@att.net | (501) 326-5167

PROFESSIONAL SUMMARY

Vice President; Cybersecurity Consulting | Consulting CISO | Director of IT Security, Data Privacy, and Compliance | Quality | Principal – Risk Management/Chief Security Officer/Chief Information Security Officer/LEAN Consultant | Director of Security and Compliance | Program Manager – Assistant Special Agent in Charge | Cyber Program Manager – Supervisory Special Agent | Project Manager | Special Agent | Manufacturing and Automation Engineer | Nuclear Engineering Officer

34 Years of Experience in Executive Leadership | Strategic Risk Management | Cyber | Critical Infrastructure Protection | Quality | Counterterrorism | Counterintelligence | Criminal Investigations | Project Management | Manufacturing Engineering | Electrical Engineering | *TS/SCI with Full-Scope Polygraph – not current*

EDUCATION

PhD Candidate, Electrical Engineering, University of Arkansas – Fayetteville, projected graduation 2025
Affiliated with NCREPT-National Center for Reliable Electrical Power Transmission.
Masters level graduate studies, Systems Engineering, University of Arkansas – Little Rock, 2014-2015
Masters level graduate studies, Electrical and Computer Engineering, Marquette University, 2001
Masters level graduate studies, Electrical and Computer Engineering, Virginia Polytechnic University, 1998
U.S. Naval Officer Nuclear Power School, 1991
U.S. Naval Officer Candidate School, 1989
Bachelor of Science, Electrical Engineering, John Brown University, 1989

SKILLS SUMMARY

- Incident Response
- Cyber Investigations
- Internal Investigations
- NIST 800-53
- Security Policy
- Governance - GRC
- ISO 27001 Certification
- COBIT
- Cloud Security
- Google Cloud Platform
- AWS Security
- Salesforce Security
- ISO 27017 & 27018
- CCPA/GDPR
- Third Party Vendor Security Management
- Internet of Things (IoT)
- NERC CIP Compliance
- NERC 693 Compliance
- FFIEC/NASAA/SEC
- HIPAA Compliance
- HITrust Certification
- Security Architecture
- Electrical Engineering
- Physical Security
- Network Architecture
- Security Risk Assessment
- Threat Assessment
- Sarbanes-Oxley (SOX)
- Secure SDLC Life Cycle
- NIST Malcolm Baldrige Quality Criteria
- NIST Malcolm Baldrige Cyber Security Criteria
- Lean Six Sigma
- 5S plus Safety/6S
- ISO 9001
- Operational Technology Cybersecurity
- Disaster Recovery/Response
- Internal Controls
- Power Engineering
- Solar Power (PV) Engineering
- FISMA/DIACAP
- Enterprise Architecture
- Data Architecture
- PCI Compliance
- Systems Engineering
- Digital Analysis
- Electronic Evidence
- Fraud Detection and Investigation
- Industrial Control Systems/SCADA
- FERPA Compliance
- Operating Systems
- Intellectual Property Rights
- Insider Threat
- Economic Espionage
- Intelligence Analysis
- Industrial Automation
- Nuclear Engineering

LEADERSHIP AND RISK MANAGEMENT EMPLOYMENT HISTORY

Vice President, Security Consulting/Managed Services
ExtraHop Networks, LLC;
April 2021 to Current, Remote

Vice President of Security Response Services for the enterprise leader in cloud-native network detection and response. Works directly with ExtraHop customers across multiple sectors including finance, healthcare, retail, manufacturing, energy & utility, and government, providing executive level direction in response to complex cybersecurity incidents. Responds rapidly and ensures compliance with regulatory frameworks including NERC, SEC, HIPAA, PCI-DSS, ISO, GDPR and CCPA. Advises customers on risk management and mitigation strategy. The practice includes cyber threat and risk assessment, incident response, internal investigations, critical infrastructure protection (CIP), regulatory compliance, disaster recovery, strategic risk management, and business continuity planning. Increased year over year sales of Advisor Consulting Services by over 480%. Increased customer base by over 310%. Increased revenue recognition by over 360% over previous year.

Consulting/Remote Chief Information Security Officer
United Capital Financial Advisors; a Goldman Sachs subsidiary
September 2017 to April 2021, Remote/Little Rock, AR

Leading and directing the FFIEC and ISO 27001 Certification for a nationwide wealth management enterprise. Developing and implementing strategies to ensure FFIEC, NASAA, and SEC Cyber-Security compliance, reduce cyber vulnerabilities, ensure availability of all wealth management applications, including Salesforce CRM. Managing multiple security technology implementation projects and vendors, including Okta, DUO, Greathorn, Fair Warning, Better Cloud, and others. Implementing robust Cloud Security Controls across multiple SaaS, PaaS, and IaaS platforms, including AWS, Heroku, Azure, G-Suite, and Salesforce, for a distributed, nationwide environment. Third Party Vendor Management (Security/Compliance). Creating and maturing all Information Security Policies, leading Cyber Security team, coordinating Cyber Security Architecture, and establishing security baselines, including Network Infrastructure Components, such as Firewalls, SIEMs, and IDS/IPSs. Achieved successful ISO 27001 Certification in June, 2019. Addressed all cyber risk management, including disaster recovery and business continuity, and due diligence issues during the 2019 acquisition of United Capital Financial Advisors by Goldman Sachs. Managed the 2019-2020 CCPA integration of United Capital into Goldman Sachs national CCPA compliance efforts.

Principal, Risk Management and Engineering Consultant, CSO/CISO - 1099
December 2015 to April 2021, Little Rock, AR

Chief Security Officer/Chief Information Security Officer for Eagle Technology, Inc., a leading Enterprise Asset Management application. Project Manager for a $3M+, 5 Year, implementation of Eagle Proteus EAM for Fortune #12 customer in a highly regulated environment. Developed Strategies to mitigate and minimize clients' institutional risk. Competencies included Cyber Security, Regulatory Compliance, Physical Security, Threat and Risk Assessment, Project and Program Management (Security and IT Security Implementations), Integrated Secure Architectures, Incident Response, Disaster Recovery and Business Continuity Planning, and Critical Infrastructure Protection.

Retained as Chief Risk Management Officer for iDatafy, a unique provider of risk mitigation services to online educational institutions.

Senior Consultant with International Performance Alliance Group, an international consulting consortium with a focus on manufacturing, LEAN, Six-Sigma, and 5S plus Safety.

Senior NIST Malcolm Baldrige Quality Examiner for the State of Arkansas Governor's Quality Award (current).

Founder and Principal Partner of LBL Compliance Consulting, providing consulting services for NERC CIP and NERC 693 standards compliance.

Senior Auditor/Assessor for the Vendor Security Alliance.

Director of Information Security and Compliance, Washington Regional Medical System
December 2016 to October 2018, Fayetteville, AR

Led and directed the Information Security, Data Privacy, and Compliance Department for a large regional healthcare and hospital system with over 30 facilities. Developed and implemented strategies to ensure HIPAA and PCI-DSS compliance, reduce cyber vulnerabilities, ensure availability of all medical record systems, and mitigate critical infrastructure threats. Project Management of 11 different security technology implementation projects, including a SIEM, IDS/IPS, network segmentation, Firewalls, Identity Management, and others. Investigated internal violations including fraud, ensuring HIPAA compliance, and ensuring analysis and review of security logs. Third Party Vendor Management (Security/Compliance). Wrote and updated all Information Security Policies. Led Cyber Security team, coordinated Cyber Security Architecture, and established security baselines, including Network Infrastructure Components, such as Firewalls, SIEMs, and IDS/IPSs. Author of multiple sections of the State of Arkansas Malcolm Baldrige Award for Excellence application. Increased the HITrust score for the system by 37% or 37 points.

Director of Security and Compliance, Southwest Power Pool
August 2015 to December 2015, Little Rock, AR
Led and directed the Security and Compliance Department for a Regional Transmission Operator/ Independent System Operator (RTO/ISO), a federally regulated electrical power generation, transmission, and distribution consortium spanning 15 states. Developed and implemented strategies to ensure NERC compliance, reduce cyber vulnerabilities, ensure electrical power reliability, and mitigate critical infrastructure threats. Investigated internal violations, including fraud, ensure SOX compliance, ensure analysis and review of security logs. Led Cyber Security team, and coordinated Cyber Security Architecture and established security baselines, including Network Infrastructure Components, such as Firewalls, SIEMs, and IDS/IPSs.

Program Manager, Assistant Special Agent in Charge
Office of the Inspector General, U.S. Department of Education
January 2015 to August 2015, Washington, D.C.
Led and directed the DOE OIG's Technology Crimes Division. Developed and implemented nationwide strategies to mitigate cyber threats to DOE networks and systems and mitigate systemic threats to federal student aid systems. Supervised and managed criminal and internal investigations involving computer intrusions and computer misuse including attacks on DOE systems (including DDOS). Managed all DOE OIG Computer Forensics. Supervised investigations of cyber threats to all DOE cyber assets nationwide, including response to audits and review of all audit logs. Coordinated Cyber Security monitoring architecture and response with DOE Security Operations Center.

Program Manager, Assistant Special Agent in Charge, Federal Bureau of Investigation
December 2010 to January 2015, Little Rock, AR
Led and directed 45 FBI Special Agents, Intelligence Analysts, and investigative support personnel. Directed, managed programmatically, and provided executive level leadership for all FBI National Security Matters in the State of Arkansas, including Cyber Crimes, Counterterrorism, Critical Incident Response, Computer Forensics, and other Technical Programs. Developed statewide strategies to address criminal, cyber, foreign intelligence, and terrorist threats impacting the State of Arkansas. Developed metrics to assess the effectiveness of operational programs. Credited with the most effective domestic terrorism program in the nation.

Program Coordinator, Supervisory Special Agent, Federal Bureau of Investigation
February 2005 to December 2010, Detroit, MI
Directed, managed, and supervised investigations of computer misuse, computer intrusion, national security related computer intrusion, economic espionage, intellectual property theft, system attacks (including DDOS), and copyright infringement. Developed strategies to address cyber-crimes statewide in the State of Michigan. Managed all computer forensics matters. Coordinated multiple Cyber Task Forces. Achieved two consecutive perfect annual program scores, indicating a noteworthy and outstanding cyber program recognized nationwide.

Project Manager, Supervisory Special Agent, Federal Bureau of Investigation
November 2002 to February 2005, Washington, D.C.
Directed, managed, and led the execution of two multi-million-dollar enterprise Information Technology projects, as the Deputy Technical Project Manager. Responsibilities included Security Architecture, establishment of a security baseline, Data Architecture, and integration into the Enterprise Architecture.

Program Coordinator, Special Agent, Federal Bureau of Investigation
July 1995 to November 2002, Washington, D.C. and Milwaukee, WI
Conducted investigations of computer intrusions, computer fraud, government fraud, and financial institution fraud. Provided numerous public presentations and seminars related to infrastructure protection, information assurance, and network security. Received extensive training in Computer Intrusions, Incident Response, and Disaster Preparedness. Conducted counterintelligence and counterterrorism investigations. Conducted classified technical operations related to national security objectives. Program Coordinator for the Milwaukee Division Cyber Crime Program and National Critical Infrastructure Protection Program. Coordinator for Cyber Crime Task Force-Milwaukee Field Office.

Consulting System Engineer, Manufacturing Automation Engineer, Electronic Data Systems
September 1994 to June 1995, Detroit, MI
Responsible for system integration, controls applications, and process application design for vehicle assembly automation at General Motors. Programmed and networked Industrial Control Systems (ICS) including programmable logic controllers and SCADAs. Designed a Graphic User Interface (GUI) oriented Computer Aided System Engineering (CASE) tool using Visual Basic. The CASE Tool was utilized for programming of Programmable Logic Controllers, manufacturing conveyer systems, and other automated manufacturing processes. Networked distributed manufacturing ICSs to the GM enterprise network.

Lieutenant, Nuclear Engineering Officer, Reserve Intelligence Officer
United States Navy and Naval Reserve
June 1988 to September 1994, Newport News, VA; Reserve Duty 1998 to 2003, Ft. Sheridan, IL
Active Duty Naval Officer, serving during Just Cause and Desert Storm. Led and managed personnel, operational, and maintenance responsibilities for a Naval Nuclear Propulsion Plant, including supervising over 20 highly trained electronic, electrical, and mechanical technicians. Managed testing, refit, and maintenance of a $183 million nuclear propulsion plant during refueling and overhaul (USS Enterprise; 1990-1994). As Special Assistant to Base Civil Engineer, expedited rollout of base enterprise network at Norfolk Naval Base (1994). Reserve Intelligence Officer specializing in Maritime Counterterrorism and Counter-Intelligence collection and analysis. (Ft. Sheridan Joint Regional Intelligence Support Center)

CERTIFICATIONS

Certified Information Systems Security Professional (CISSP), #567714, July 2016
NSA-Committee for National Security Systems (CNSS) 401, 2007
FBI Computer Intrusion Investigator, 2001
State of Arkansas Malcolm Baldrige Governors Quality Award Senior Examiner
NIST Department of Commerce National Malcolm Baldrige Performance Excellence Award Examiner
Member of ISC2, ISACA, PMI (Project Management Institute), and the IEEE.

EXHIBIT A-4

Affidavit of Mark Daniel Bowling

State of Arkansas
County of Saline

COMES NOW Mark Daniel Bowling, being first duly sworn, under oath, and states that the contents of the following attached reports, including their appendices, and exhibits are true and correct statements of relevant facts and his opinions in the case of United States v. Keith Raniere et. al., in the United States District Court, Eastern District of New York, Case #: 1:180-cr-00204-NGG-VMS, to the best of his knowledge and belief:

- Summary of Technical Findings, dated December 13, 2022

Signature: _____

Address: 33 Sosegado Lane
Benton, AR 71909

SUBSCRIBED AND SWORN TO before me this 13 day of December, 2022, by Mark Daniel Bowling.

Jennifer C. Dorsey
NOTARY PUBLIC FOR ARKANSAS

JENNIFER C. DORSEY
OFFICIAL SEAL - NOTARY PUBLIC
GARLAND COUNTY ARKANSAS
COMMISSION #12716295
MY COMMISSION EXPIRES 9-22-2031

My Commission Expires: 9/22/31

Mark Daniel Bowling, CISSP

FBI Special Agent and OIG Investigator (Retired) and Consulting CISO

December 13, 2022

Summary of Technical Findings

Professional Background

I served as an FBI Special Agent for ~ 20 years, from 1995 to 2015, and as an Office of the Inspector General Special Agent for ~ 1 year, during 2015. The balance of my investigative career was in cybersecurity investigations, with some experience in digital forensics. In service with both the FBI and the OIG I served as a case agent, a field supervisor, a Cyber Program Manager, a Senior Supervisory Resident Agent, an acting Unit Chief, a Technical Project Manager, a forensic examiner, an acting Assistant Section Chief, an Assistant Inspector in Place, and as an Assistant Special Agent in Charge. I have an in-depth knowledge of FBI and OIG digital evidence examination procedures, Federal investigative operational policies and procedures, and the inspection and auditing of the execution of those policies and procedures.

Review of Evidence

On September 12, 2022, I signed the Protective Order Regarding Discovery in U.S. v. Raniere, et al., 18 CR 204 (NGG) and was subsequently provided access to certain evidence in this case. My review of evidence includes court testimony, a hard drive copy of logical files, and examination reports generated by members of the FBI's Computer Analysis Response Team (CART).

The primary intention for the review of this evidence was to technically recreate, and thus empirically validate or refute, any or all of the seven Technical Findings previously identified and documented by Dr. J. R. Kiper. Any additional findings, technical determinations, and logical conclusions were also documented. In executing this examination, I reviewed portions of forensic reports **GX 521A_Replacement.pdf** (the second FBI CART's FTK report for the CF Card) and **GX 505A.pdf** (the FBI CART's FTK report for the WD HDD), and forensically examined specific files in the two forensic duplicate images of **GX 521A** (the CF Card) and **GX 505A** (the WD HDD).

Summary of Findings

Based on my review, I determined specific actions had been taken to falsify the evidence, in support of the government's narrative that photos were taken by a Canon EOS 20D camera (GX 520), saved to a Lexar CF card (GX 524), copied to an unknown computer, and then backed up to a Western Digital hard disk drive (GX 503). In this report, I referred to the latter two items as the CF Card and the WD HDD.

In my 20 years as an FBI Agent, an FBI Assistant Inspector, and an OIG Agent, I have personally investigated and have been made aware of multiple instances of FBI misconduct. These include intentional misconduct by executives, misconduct by supervisors, and misconduct by field agents. I am

aware of one event where an FBI CART examiner allowed for the negligent destruction of original digital evidence.

However, until this case, I have never previously become aware of, personally investigated, or researched an instance of an FBI CART examiner and/or other FBI personnel willfully, intentionally, or maliciously falsifying digital evidence.

In this case, I conducted an independent validation of the Technical Findings #1 thru #7 from Dr. Kiper. I concur with his findings.

- It is a complete technical certainty that much, if not all, of the digital evidence, including both the WD HDD and CF Card, was manipulated prior to analysis, and possibly manufactured.
- It is factually certain that the FBI violated numerous digital evidence examination procedures, and that the second FBI CART examination of the CF Card was both in violation of FBI policy and did not conform to best digital examination practices.
- It is also certain that evidence tampering occurred on the CF card while it was exclusively in the custody of the FBI and that the FBI mishandled that item of the digital evidence.

EXHIBIT A-5

William Odom
Co-Founder
Orbital Data Consulting

Contact information
Office: +1 346-352-8876
Direct: +1 713-927-5377
Email:wfo@orbital.global
Website: https://orbital.global/

LinkedIn profiles:
www.linkedin.com/in/williamodom

www.linkedin.com/company/orbital-data-consulting/

William Odom has over 25 years of experience in computer forensics, cybersecurity investigations, electronic discovery, and expert testimony globally. He is a Co-Founder for Orbital Data Consulting, where he leads the global team for Digital Forensic and Incident Response investigations. He began his career in this area as a Special Agent with the FBI where he received training in general investigative techniques, computer intrusion and security matters and national intelligence and counterintelligence matters. He was also certified through the FBI Laboratory as a Certified Computer Forensics Examiner for the FBI's Computer Analysis Response Team (CART). During his service, he managed the Computer Forensics Lab for the Houston office of the FBI and was involved in nearly all the 200+ federal matters investigated by the FBI, ranging from white-collar crime to terrorism and national security matters.

His experience includes cybersecurity breaches and intrusion investigations, electronic discovery, forensic computer science, information security and data analysis experience. He has significant expert testimony experience related to computer forensics, written numerous affidavits and managed the collection of thousands of computers, network and mobile devices. He routinely consults with clients regarding electronic discovery matters, such as helping clients prepare for discovery by assessing sources of Electronically Stored Information ("ESI") and designing preservation and collection protocols. He has directed the preservation, analysis, and review of ESI in a range of matters including intrusion and criminal investigations, independent litigation, regulatory compliance, and internal inquiries.

He has led numerous projects for Fortune 500 companies and their counsel. His experiences in these matters cover numerous industries, including Oil and Gas, Automotive, Financial Services, Healthcare, Consumer Products, Technology, Retail, and Manufacturing.

Following is a list of William's general case work and representative engagements.

General Case Work:

- Has testified as an expert witness and provided expert opinion in state and federal court in matters in civil, administrative, and criminal courts in the US as well as in France

- Former CISO of Forensic Risk Alliance where he directed strategy, operations, and the budget for the protection of the enterprise information assets and manages that program on a global scale. My responsibilities encompassed communications, applications, and infrastructure, including the policies and procedures that applied.

- Has led teams and conducted analysis on internal and external intrusion investigations and assisted with identification and remediation of stolen or affected data. Has identified intrusion source(s) and assisted with both civil remedies and criminal prosecution of responsible parties

- Has led teams on numerous preservations, collection, and computer forensic investigations into theft of trade secrets and confidential company information by current or departing employees, with subsequent findings resulting in action against former employees, including termination and damages.

- Has provided lead technical expertise in multiple engagements dealing with the analysis of data and hardware from several architectures and file systems including re-creating file system structure from software RAID and logical volumes, backup tape analysis, and hard drive analysis.

- Has led multiple engagements in forensic imaging and evidence gathering procedures, detailed examinations, and client production for sensitive, corporate investigations involving employees, owners, and/or investors, in many areas of industry. Provides electronic evidence collection and investigative services to corporate entities directly or through external counsel in highly confidential and sensitive matters.

- Has led numerous restoration projects of data from backup tape or backup systems where traditional means of restoration by internal IT or other experts had failed. Has experience with numerous backup tape hardware and software, historical operating systems, and hardware, as well as recreating unique environments in order to successfully restore data considered by IT professionals or other experts to be unworkable.

- Has directed, managed, and executed multiple engagements on behalf of counsel in support of their clients dealing with the forensic technology component of SEC reporting issues. He has provided guidance and support on these engagements in computer forensics, large-scale data collections, and electronic discovery and document productions to third parties, including US and foreign government agencies.

- Has provided guidance and led multiple electronic data related engagements includes the planning, interviewing of clients' IT personnel, data transfer, database development, testing, and reporting. I regularly manage the transfer of knowledge between corporate personnel, both technical and non-technical, counsel, forensic accountants, and other investigative personnel.

Representative Cases:

- Appointed as a neutral expert in a Federal theft of intellectual property matters. Executed civil seizure orders (in conjunction with the U.S. Marshall Service) as well as subsequent analysis and testimony to the court.
- Led a cyber intrusion investigation in Colombia for a large government partnered organization related to a large-scale interruption of business services.
- Analyzed computer evidence for a large oil and gas company, including hundreds of backup tapes and dozens of computers, to determine if evidence destruction occurred as part of an ongoing civil litigation. Successfully testified that no spoliation occurred.
- Investigated and testified on the creation of a fraudulent email that was created for the purpose of misinformation in a civil litigation.
- Investigated computer evidence for oil and gas company for evidence of intrusion. Determined that intrusion was from "trusted" source.
- Executed a civil search warrant for a Fortune 500 corporation and managed the subsequent forensic analysis of electronic evidence related to theft of proprietary information.
- Located evidence of theft of intellectual property from a company computer by one administrative user. This evidence was traced to a competitor and was located on over 50 computers in their facility.
- Testified in court as an expert for the plaintiffs in a Federal Civil Matter regarding wire-tapping charges by the City of Providence, RI. Jury ruled in favor of plaintiffs for 58 million dollars in damages.
- Analyzed digital evidence and expert reports in a criminal matter regarding email fabrication by a user in a separate civil matter. Ultimately provided evidence that suggested the defendant did not produce the fake email and all criminal charges were dropped.
- Managed a litigation matter that involved the imaging and analysis of approximately 130 computers and the recovery of e-mail and electronic documents from 400 backup tapes.
- Managed a forensic preservation of 110 computers in the US and Mexico that was successfully completed in less than 3 days.
- Analyzed and recovered deleted data that led the successful recovery of a runaway teenager.
- Managed preservation and computer forensic matters globally, in the following countries: The United States, Canada, Mexico, Colombia, Brazil, Honduras, Australia, Japan, Indonesia, China, Morocco, Nigeria, Belgium, The Netherlands, Ireland, England, France, Germany and the Czech Republic.
- Involved in execution of several search warrants as ordered by the court of the Foreign Intelligence Surveillance Act. The nature of these national security matters requires surreptitious entry and security countermeasures.
- Trained law enforcement and private industry, in United States and abroad, on computer forensic and intrusion matters.

Prior Work Experience

- Current – **Co-Founder** for **The Orbital Group**, where he lead all digital forensic and incident response investigations.
- 2018 to 2019 – Director and Acting CISO for **Forensic Risk Alliance** for the Digital Forensic Team.
- 2014 to 2018 – Senior Manager for **Ernst & Young** in the Forensic Technology & Dispute Services team of Ernst & Young's Fraud Investigation and Dispute Services (FIDS) practice in Houston, TX. William was the America's Leader for all digital forensic collections and investigations.
- 2012 to 2014 - Senior Managing Director for **D6 Consulting**. William led the Houston digital forensic and eDiscovery practice for D6 Consulting.
- 2010 to 2012 – Owner and lead investigator for **Digital Forensic Excellence** in Houston, TX.
- 2007 to 2010 – Managing Director for **StoneTurn Group** of Forensic Technology Services in Houston, TX.
- 2005 to 2007 – Adjunct Instructor for **Sam Houston State University** in Huntsville, TX. Created and taught Graduate level digital forensic curriculum as well as created and taught digital forensic and incident response training for local, state, and Federal law enforcement.
- 2003 to 2007 – Principle/Director of Digital Forensic Services for **Acquisition Data/Integrity Partners** in Houston, TX.
- 2001 to 2003 – Manager for **Deloitte Financial Advisory Services LLP** in Houston, TX specializing in Forensic Technology, Collections and Analytics.
- 1996 to 2001 – Special Agent for the **Federal Bureau of Investigation** (FBI) in New York, NY and Houston, TX. William was certified by the FBI as both a Computer Analysis Response Team (CART) Computer Forensic Examiner and as a Computer Crime Investigator.
- 1991 to 1996 – Computer programmer in Dallas, TX.

Publications

- Phishing for Facts: Managing and Preventing Fraud and Cyber Risk is Simply about Preparation
- The Importance of Memory Forensics in Fraud Investigations

Education & Certifications

- Bachelor of Science with a double major in Computer Science & Mathematics from the University of Southern Mississippi in 1990.
- Federal Bureau of Investigation – Completed New Agent Training in Quantico, VA in 1996
- Federal Bureau of Investigation – Advanced Computer Intrusion Detection and Countermeasures - 1998
- International Association of Computer Investigative Analysts – Basic Computer Forensic Certification in 1998
- Federal Bureau of Investigation – Basic Computer Forensics Certification in 1998
- Federal Bureau of Investigation – Advanced Computer Forensics Certification in 1999
- International Association of Computer Investigative Analysts – Advanced Computer Forensic Training in 2000
- Federal Bureau of Investigation – Instructor Development Course in 2000

- Federal Bureau of Investigation – Basic and Advanced UNIX Forensics Certification in 2000
- Federal Bureau of Investigation – Macintosh Computer Forensics Certification in 2001
- Federal Bureau of Investigation – IBM AS/400 Computer Forensics Certification in 2001
- EnCase Enterprise Acquisition Training in 2002
- EnCase Training in 2003
- Stegonagraphy and Malware Training in 2004
- EnCase Certified Examiner (EnCE) in 2004
- AccessData Forensic Boot Camp Training in 2004
- AccessData Internet Forensics Training in 2005
- AccessData Windows Forensics Training in 2005
- WetStone Technologies Stegonagraphy Certification in 2005
- iConnect / XERA Administration Certification in 2013

EXHIBIT A-6

Affidavit of William F. Odom, III

State of Texas
County of Harris

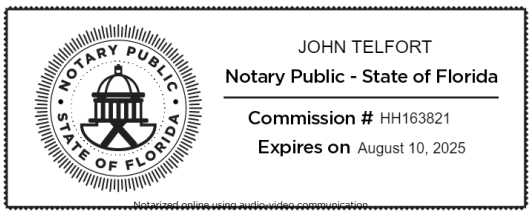
COMES NOW William F. Odom, III, being first duly sworn, under oath, and states that the contents of the following attached reports, including their appendices, and exhibits are true and correct statements of relevant facts and his opinions in the case of United States v. Keith Raniere et. al., in the United States District Court, Eastern District of New York, Case #: 1:180-cr-00204-NGG-VMS, to the best of his knowledge and belief:

- DIGITAL FORENSICS FINDINGS REPORT (December 20, 2022)

Signature: William Odom

Address: 9815 Darby Mill Lane
Houston, TX 77095

SUBSCRIBED AND SWORN TO before me this 21st day of December, 2022, by John Telfort.



NOTARY PUBLIC

My Commission Expires: 08/10/2025

DIGITAL FORENSICS FINDINGS REPORT

Summary of Findings Regarding Digital Evidence Utilized in U.S. v Raniere, et al.

20 December 2022

TABLE OF CONTENTS

BACKGROUND AND ENGAGEMENT DETAILS

My name is William F. Odom, III and I have over 25 years' experience in computer forensics, cybersecurity investigations, electronic discovery, and expert testimony globally. I am a Co-Founder for Orbital Data Consulting Group, LLC ("Orbital"), where I lead the global team for Digital Forensic and Incident Response investigations. Orbital is a Digital Forensic, eDiscovery and Cybersecurity consulting firm with offices located in both the US and Europe. I began my career in this area as a Special Agent with the FBI where I received training in general investigative techniques, computer intrusion and security matters and national intelligence and counterintelligence matters. I was also certified through the FBI Laboratory as a Certified Computer Forensics Examiner for the FBI's Computer Analysis Response Team (CART) and served both in the New York and Houston Field Offices. During my service, I was involved in nearly all the federal matters investigated by the FBI, ranging from white-collar crime to terrorism and national security matters. I was also an adjunct instructor of Digital Forensics at Sam Houston State University, where I both created and taught basic and advanced Digital Forensic courses to both law enforcement and university students alike. I have testified as an Expert Witness in both Criminal and Civil matters throughout the U.S. in both State and Federal level courts. I have also presented Expert Testimony in the French court system. My CV is attached as Exhibit A for reference.

In late September, Orbital was engaged by the legal defense team to review analysis previously performed and reported on by Retired FBI Agent J. Richard Kiper, PhD, PMP , as well as to conduct an independent data analysis of digital evidence related to the referenced matter, U.S. v Raniere, et al. In particular, Orbital was asked to provide an unbiased opinion as to whether or not there were irregularities with the digital evidence presented by the FBI during trial against Mr. Rainere as well as the process utilized by the CART examiners. The results of the analysis performed by Orbital and Mr. Odom are detailed below.

EVIDENCE LIST

Orbital was provided access to affidavits generated by Dr. Kiper on both technical and procedural concerns as well as court testimony, a hard drive

containing logical files and examination reports generated by members of the FBI's CART.

ANALYSIS AND FINDINGS

In Dr. Kiper's Affidavit dated April 25, 2022, he provides several findings related to the actions taken by the FBI's CART to manually alter digital evidence to further a narrative that specific digital photos containing an underage female were taken by a Canon EOS 20D camera containing a Lexar CF storage card, copied to an unknown computer where it was backed up to a Western Digital hard drive. For the purposes of this findings report, I will utilize the same wording and order as Dr. Kiper and his seven key findings to provide Orbital's analysis results.

1. Some digital photos found on the Lexar storage card had the same filenames and date/time stamps as files found on the Western Digital hard drive, yet they depicted two different people. Moreover, these same Lexar card files contained thumbnail pictures from another existing set of photos, thus proving that manual alteration of the Lexar card contents.
    a. Orbital reviewed Dr. Kiper's explanation that these images were manually altered on the Lexar card and Western Digital hard drive, and I agree with his findings that these files appear to be manually altered.
    b. Orbital performed an independent review of the same data identified here and were able to recreate the same results.
    c. I agree that these digital photos appear to have been manually altered, as identified by Dr. Kiper.
2. Additional files appeared on the FBI's forensic report of the Lexar card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the Lexar card and the Western Digital hard drive.
    a. Orbital reviewed Dr. Kiper's explanation and I agree that there are discrepancies between the two FBI reports.
    b. I also reviewed the reports and noted the same discrepancies.
    c. I agree that this inconsistency between reports is not expected behavior and does appear as an anomaly. Dr. Kiper noted that the

same version of the forensic software (Forensic ToolKit, ver. 6.3.1.26) was used to generate both FBI forensic reports. I am familiar with this software and I have never experienced any software issue or glitch that itself could explain the appearance of new files. Given the evidence available to me for review, I agree that that newly appearing files on the second report were likely from an attempt to create a stronger relationship between the Lexar card and the Western Digital hard drive

3. An unknown person accessed the Lexar card on 9/19/18, thereby altering file system dates, while this card was in the custody of FBI Special Agent Michael Lever.
    a. Dr. Kiper noted that SA Lever checked out the camera and camera card on 9/19/18 from Evidence Control for the purposes of review. Further, the Last Accessed date for all the active files was updated to 9/19/18, which is consistent with the date that the card was in possession of SA Lever. As noted, it is against FBI policy to access original evidence without a write blocker to prevent such alterations to the original evidence.
    b. While we don't know precisely how the Last Access dates were altered, the timing of these dates on all the active files is consistent with the Lexar card being accessed without any type of write-blocking device to protect this access while in FBI custody and control.
    c. I agree that it appears that these files were accessed through some means that updated the Last Access times on all active files on the Lexar card and that this is against FBI policy.
4. Dates of photos on the hard drive were altered through manual intervention. The alterations seem to be an attempt to alter dates and, in doing so, account for Daylight Savings Time.
    a. Dr. Kiper describes his analysis of specific files that it appears that some manual intervention occurred in an attempt to adjust specific data to account for Daylight Savings Time. He further states that based on the evidence he has available, he does not have a legitimate reason a normal user would be making similar changes.
    b. I agree that, based on the information available, there is no legitimate or easily explainable reason why these particular files, or

any files, would have their Modified dates altered in such a fashion. I agree that these observed timestamp inconsistencies appear anomalous, and are consistent with manual manipulation.

5. The metadata of a modified photo, whose numbered filename appears between the alleged contraband ranges, was manually altered to create the appearance that it had not been modified.
    a. Dr. Kiper identified that for one image on the Western Digital hard drive, named IMG_0175, that the Modified date matches the same file name on the Lexar card. However, the EXIF data for this file indicates that it was created by “Adobe Photoshop Elements”. Dr. Kiper further notes that the thumbnail data associated with this file is inconsistent with other thumbnail data from similar files. His conclusion is that this file was manually altered and that whoever altered this file likely forgot to clean up the EXIF data to hide their impropriety.
    b. I agree with Dr. Kiper that this file could not have resulted just from being taken the Canon camera from which it was supposedly taken. My own analysis confirms that Adobe Photoshop Elements is software that is run from either a Windows or Mac computer. In a review of the photos that are available for me and were purportedly taken by the Canon camera, the EXIF data identifies the Canon EOS 20D as the creator. The fact that this specific photo contains the EXIF data stating that was created by “Adobe Photoshop Elements”, along with the inconsistency of the carved thumbnail data, I agree with Dr. Kiper that this photo was manually altered. I agree that, in light of these indicators of manual alteration, the fact that the Modified date matches the EXIF creation date appears anomalous and is consistent with manipulation of the Modified date metadata.
6. The folders containing the alleged contraband and others that supported the dating of the photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.
    a. Dr. Kiper contends that the naming convention of the folders on the Lexar card is inconsistent with how the camera saves pictures in folders to a storage card, but that it is consistent with the naming

convention of Adobe Photoshop Elements. Further, these folder names were altered to appear to be created during the timeframe of when the pictures were allegedly taken by the Canon camera.

b. I agree with Dr. Kiper that this naming convention and the related evidence does appear anomalous, and it is consistent with manual manipulation. I agree Dr. Kiper that based on the evidence available, these folder names do appear to have been manually manipulated and that, at the very least, the dates and times in these folder names cannot be relied upon to determine or corroborate the creation dates of the photos contained within. I agree that the thumbs.db anomaly identified by Dr. Kiper in relation to the two folders ("2005-10-19-0727-59" and "2005-10-19-0727-57") is further indication these folder names, and folder content, were manually altered.

7. The photos in this case, including the alleged contraband photos, appear to be on the hard drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates.

a. Dr. Kiper contends that the contraband images contained on the Western Digital hard drive appear to have been manually stored there to appear to have come from an automated backup from an unknown computer or computers. He notes inconsistencies in the create dates of the files in this backup, as well as the file sizes. Further, he contends that it appears that if someone manually rolled back a computer clock to appear as if the backups were created at an earlier time; specifically in 2009.

b. Since neither the government, nor anyone else, has unknown computers from which any automatic backups could have been created, it is difficult to verify if such a backup occurred in 2009. However, based on the evidence that is available, I agree with Dr. Kiper that there are inconsistencies with the backup dates and there is evidence to suggest that the contents of the alleged backup were placed there manually, with manipulated dates, rather than through an automated process.

SUMMARY OF FINDINGS AND OBSERVATIONS

Orbital reviewed a large amount of data, including affidavits, courtroom testimony, reports created by FBI CART examiners and a logical copy of evidentiary data. We were not able to review the original evidence seized by the FBI, as it is in their custody and control, and it allegedly contains contraband information. As such, my opinions are based on what information and data is available to me, as well as my understanding of digital forensics and the related processes.

Based on my training and experience, I agree with Dr. Kiper's findings, in that certain digital evidence presented in trial by the FBI against Mr. Raniere appears to have been manually created and altered by a person or persons unknown. Furthermore, this evidence manipulation appears to further the government's narrative that the contraband images were taken from a digital camera seized from the defendant.

I also agree that the general processes utilized by the FBI and/or person or persons unknown, including general chain of custody procedures and write blocking technology, were not appropriately managed and do not adhere to either FBI policy or general digital forensic best practices.

I do not see a reasonable nor plausible explanation for these inconsistencies in the digital evidence. As such, it is my opinion that digital evidence was altered while in FBI control and that such altered evidence was presented in court against Mr. Rainere in the case U.S. v Raniere, et. al.

Orbital reserves the right to supplement these findings as new evidence is made available.

William Odom

William F. Odom, III
Co-founder

Dated: December 20, 2022

EXHIBIT A-7

Appendix C

Curriculum Vitae of Stephen Michael Bunting

Bunting Digital Forensics, LLC • 33579 Blue Heron Drive • Lewes, DE 19958
Phone: +1.302.260.2633 • E-Mail: stephenbunting@mac.com

Summary of Experience

Mr. Bunting is an experienced digital forensics examiner who is CEO and Senior Forensic Consultant of Bunting Digital Forensics, LLC. He also works as the Senior Manager of Services for SUMURI, LLC as an independent consultant. Formerly Mr. Bunting was a Manager with Alvarez & Marsal (Sept 2012 to Feb 2013) and prior to that a Senior Forensic Consultant with Forward Discovery (Sept 2009 to Sept 2012). (Alvarez and Marsal acquired Forward Discovery in Sept 2012) His responsibilities with Bunting Digital Forensics, Alvarez & Marsal, and Forward Discovery include:

- Acquisition and forensic examination of digital media using industry standard forensics tools;
- Develop & instruct classes on Windows, Macintosh and Mobile Device Forensics;
- Develop & instruct classes on cyber investigations and related course work;
- Investigative consultation and digital forensics examinations in many areas including spoliation, theft of intellectual property, malware analysis, unlawful access of computer systems, theft of corporate resources, employee misuse of computer systems, Medicaid fraud, and support of various types of criminal investigations (prosecution only - no criminal defense work);
- Consult with clients and develop E-Discovery plans;
- Carry out electronic discovery data collection from a wide array of devices and services (servers, network shares, workstations, laptops, smart phones, and cloud services – while Mac is included in the terms workstations and laptops, Mac is a specialty area)
- Under sub-contract (multiple vendors) to the U.S. Department of State, develop & instruct various cyber-based anti-terrorism courses to international law enforcement agencies.
- Under Bunting Digital Forensics, instruct XRY Foundation, Intermediate, PinPoint, XAMN, and Kiosk Courses. Currently the only contract instructor for MSAB (XRY) in the U.S.
- Under Bunting Digital Forensics, instruct courses for Magnet Forensics as a contract instructor.
- Bunting Digital Forensics is under contract to SUMURI, LLC, whereby Steve Bunting manages the services division of SUMURI.

Mr. Bunting retired (August 2009) from a law enforcement career spanning over three decades during which he conducted hundreds of examinations of computer systems for the University of Delaware Police as well as federal, state, and local law enforcement and prosecutorial agencies. He is also a trained and experienced forensic video analyst using the Ocean Systems dTective® and Avid software systems. He is a frequent lecturer and instructor on computer forensics, cyber-crime, and incident response.

Mr. Bunting has testified in many trials as a computer forensics expert. He was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence for receiving the highest test score on his certification examinations. Among his varied certifications he is an EnCase Certified Examiner EnCE (Guidance Software), an AccessData Certified Examiner (ACE), Certified Computer Forensics Technician (HTCN), Certified XRY Instructor, BERLA Certified Vehicle Forensics, Magnet Certified Forensics Examiner, and X1 Social Examiner.

Mr. Bunting is a retired a police captain, having served in the State of Delaware for over thirty-five years. He created and developed the University of Delaware Police Department's Computer Forensic Lab. He has taught computer forensics for Guidance Software, makers of EnCase, and taught as a Lead Instructor at all course levels, including the Expert Series with particular emphasis on "Internet and Email Examinations" course. He has instructed students in computer forensics on an independent study basis for the University of Delaware and is an adjunct faculty member of Goldey-Beacom College, teaching computer forensics. He has been a presenter at several seminars and workshops, the author of numerous "white papers", the principle author of *EnCase Computer Forensics - The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition*, the co-author *Mastering Windows Network Forensics and Investigation* , *the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 2nd Edition,* the co-author *Mastering Windows Network Forensics and Investigation 2nd Edition, the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition* (all published by Wiley).

Recent Consulting Engagements

Mr. Bunting engages in a significant number of instructional / research endeavors as well as engaging in consulting / case work, as one augments the other. Many engagements were totally confidential, while some were public to the extent of the details found in court records. Some of those engagements are described below:

Serving as an embedded mentor with the Albania State Police beginning in 2019 and continuing through 2022, with a contract to continue through 2023. As such, spending two and three week periods, onsite, working with their existing computer forensics lab, enhancing their capabilities, and working with their Counter Terrorism Unit, starting up a brand-new computer forensics lab specific to the CT mission.

Conducted a forensic examination of computers used by a former employee and documented evidence that showed exfiltration of IP data. The exfiltrated data was used to jump start a competing business. The initial report served as a basis to shut down the competing business and bring about a settlement. The former employee did not settle and the matter went to trial, during which Mr. Bunting testified at length concerning the forensics findings.

Recovered data from an Android phone that had been underwater and was delivered 'in pieces'. Using chip-off technique, all data was fully recovered including data that had been deleted.

Served as an expert for two defendants who were facing spoliation claims. Established that opposing expert had failed to discover settings whereby SMS's messages were forwarded from an iPhone to a MacBook Pro. Opposing expert claimed SMS messages were deleted from the iPhone when in fact they were in the opposing expert's possession on the MacBook Pro. Said deletions were offered as evidence of spoliation. Opposing expert also failed to find over 11,000 AIM Messenger chats that were on the iPhone.

Served as a trusted third-party digital forensic examiner in a Virginia case where a former employee was accused of theft of intellectual property, specifically programming code. Determined that accused party provided fabricated exhibits to examine in the form of a contrived MacBook Pro in which the time had been altered to appear to contain historical data when in fact it was only 3 weeks old.

Conducted digital forensics examinations of computers believed to be involved in a telecommunications fraud in the Middle East region, whereby perpetrators were conducting a multimillion-dollar fraud in a balance-transfer scheme exploiting a software defect.

Conducts ongoing training and course development for the U.S Department of State's Anti-Terrorism Assistance Program Cyber Division. As such six to eight courses are delivered each year in varying international locations.

Ongoing consultation with a digital forensics firm that specializes in examinations for copyright infringement cases in the motion picture industry involving peer-to-peer clients to download movies and other protected media.

Ongoing consultation with a digital security company in the UAE, providing incident response support services.

Developed a new Macintosh Digital Forensics course for the Delaware State Police Child Predator Task Force. The course is an in-depth program intended for those with significant digital forensics experience. It includes a unique module entitled "Digging Deeper – Research Techniques to Establish User Culpability", which is the first of it kind.

Developed and delivered a virtual course entitled: Cyber Security Investigations: Incident Response for the FedCTE program. The course was developed for virtual delivery using the AvayaLive virtual classroom and first delivered on June 25, 2014.

Provided expert witness services establishing that the plaintiff fabricated an email submitted during discovery in a civil matter. Testified in US District Court (Princeton, NJ) as expert for defense in computer forensics analysis and email analysis in a hearing to dismiss based on fraudulent documents offered into evidence by plaintiff. Specifically, testified that document

proffered as an email was in fact fabricated to appear as such. – July 09, 2014. The matter is still under litigation.

As a member of a team, conducted an on-site assessment of a major middle east country's governmental cybercrime unit and digital forensics unit, prepared gap analysis reports, and prepared recommendations for creating ISO 17025 compliant laboratory operations, a modern cybercrime investigation and intelligence gathering unit, as well as country-wide expansion of capabilities for both units.

Assigned as principal leak investigator for a major mobile device manufacturer. Investigated significant intellectual property losses on a global basis.

Conducted a security assessment, as part of a team, of a Caribbean country's government IT infrastructure and made recommendations for securing their systems according to best practices.

Conducted computer forensic examination of all computers from a dental practice in a Medicaid fraud case. Examination involved reconstruction of a dental practice's business transactions spanning several years through analysis of SQL transaction logs from Patterson's *Eaglesoft* dental practice software. The findings in the report submitted substantiated ongoing fraud and induced a guilty plea, resulting in the incarceration of the offending dentist.

Conducted computer forensic examination of over two-dozen laptops belonging to employees of a major brand integrity unit, which investigates and mitigates brand piracy for its parent company. The unit was distributed in six countries and had been accused of various breaches of duty and unlawful acts. The examination took several months to complete and findings documented and substantiated the majority of the allegations, resulting in the dismissal of several employees.

Certifications

X1 Social Examiner	April 2019
Magnet Certified Forensics Examiner	March 2018
BERLA Certified Vehicle Forensics	September 2017
Certified XRY Instructor, MSAB (Sweden)	October 2013
Certified ACE AccessData Certified Examiner	April 2011
Certified iPhone Examiner, MSAB	November 2010
Certified XRY Complete Examiner, MSAB	October 2010
Certified LAW PreDiscovery Administrator, LexisNexis	January 2010
Certified LAW PreDisovery User, LexisNexis	January 2010

Certified Computer Forensic Technician, High Tech Crime Network	September 2001
EnCase Certified Examiner, Guidance Software	April 2002
Certified Cell Phone Examiner, Paraben Corporation,	May 2005
Certified PDA Examiner, Paraben Corporation	May 2005
State of Delaware Council on Police Training Certified Police Officer	April 1975

Employment History

SUMURI, LLC – Camden, DE – Senior Manager of Services (as independent contractor) – November 2016 to present

- Provide management services for SUMURI's Services Division
- Develop and carry out the business plan for services
- Coordinate services, match resources with service needs, and ensure quality control
- Conduct digital forensic examinations and investigations

Bunting Digital Forensics, LLC – Lewes, DE – CEO & Senior Digital Forensic Consultant – February 2013 to present

- Conduct digital forensics examinations on a variety of media, including mobile devices
- Develop training programs for various cyber related topics
- Deliver training programs as an independent contractor for the Antiterrorism Assistance Program Cyber Division (see NDI below)
- Conduct assessments of digital forensics laboratories, conduct a gap analysis, and recommend a roadmap for improvements leading to accreditation
- Conduct specialized digital forensics examinations in support of Medicaid fraud cases

Microsystemation (MSAB) – Stockholm, Sweden – Contract instructor for XRY training courses – October 2013 to present

Teach XRY Mobile Device Forensic Solutions Courses

Alvarez and Marsal, Washington, DC – Manager, Forensic Technology Services – September 2013 to February 2013

- Develop and deliver a variety of training courses, including Macintosh Forensics, Incident Response, and Advanced Digital Forensics Courses.
- Developed and facilitated a table top training exercise to test and enhance the incident response capabilities of a large web hosting company
- Conduct digital forensic examinations on media associated with compromised systems.

• Interim Management, specifically Principle Leak Investigator for a large telecommunications company experiencing a significant loss of intellectual property.

Forward Discovery, Inc – San Antonio, TX – Senior Forensic Consultant – September 2009 to September 2012

Information security company that provides digital investigation, electronic discovery, vulnerability assessments and training services to corporate and government clients.

• Acquisition and forensic examination of digital media using industry standard forensics tools

• Develop & Instruct classes on Windows, Macintosh and Mobile Device Forensics

• Develop & Instruct classes on Cyber Investigations and related course work

• Investigative consultation in areas including theft of intellectual property, malware analysis, unlawful access of computer systems, theft of corporate resources, employee misuse of computer systems, and support of various types of criminal investigations (prosecution only - no criminal defense work).

• Consult with clients and develop E-Discovery plans

• Carry out electronic discovery processing from initial acquisition to final load file

Network Designs, Inc. – McLean, VA – Senior Instructor ATA Cyber Division as an Independent Contractor – September 2009 to present. On a contract basis to NDI, work as a Senior Instructor supporting the U.S Department of State Anti-Terrorism Assistance Program's Cyber Division, which included the following:

• Develop training modules for new training programs

• Provide advisement, briefings and presentations to foreign law enforcement officers on areas including cyber terrorism and cyber crime

• Provide technical computer investigation training to law enforcement and governmental agencies worldwide. Course taught include: Identification & Seizure of Digital Evidence, Introduction to Digital Forensics & Investigations, Macintosh Forensics, Cell Phone Forensics Consultation, EnCase Software Consultation, Server Incident Response (ADFC), Fundamentals of Network Security, Cyber Unit Management Consultation Proactive Internet Investigations Course, Forensic Equipment Grant Consultation, and Digital Forensic Lab Mentoring and Consulting.

Guidance Software – Pasadena, CA – Part-time Instructor - 2004 - 2005.

- Lead instructor teaching courses at all levels (Beginning to Expert)
- Assisted in course development and review

University of Delaware Police Department – Newark DE – Captain - July 1980 to August 2009.
Principle duties were:

- Computer Forensics Unit (Founded and Managed)
- Accreditation (Accreditation Manager)
- Southern Operations (Managed)

Education

University of Delaware - Computer Applications Certificate – Concentration in Network Environments - August 2004

Wilmington College - Bachelor of Science Applied Professions / Business Management - May 1986

Delaware Technical and Community College - 52 credit hours in the Criminal Justice Program

University of Delaware - Associate in Art - May 1973

Publications

How Did That Photo Get On That iPhone? Deep Dive Into The iOS "Photos.sqlite" database: Part 1 **– MSAB Blog – (to be published) Fall 2022**

Forensic Analysis of Spoliation and Other Discovery Violations - Part 2 of a 2-Part Series - Windows Examinations - eForensics Magazine - December 2016

Forensic Analysis of Spoliation and Other Discovery Violations **- Part 1 of a 2-Part Series - Macintosh Examinations - eForensics Magazine - October 2016**

EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide**, 3rd Edition - author - Wiley - September 2012**

Mastering Windows Network Forensics and Investigation **(one of four co-authors) - Wiley - 2012**

EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide**, 2nd Edition - author - Wiley - November 2007**

Mastering Windows Network Forensics and Investigation **(one of two co-authors) - Wiley - April 2007**

Encase Computer Forensics—The Official EnCE: Encase Certified Examiner Study Guide **- primary author - Wiley - January 2006**

Memberships and Affiliations

Infragard – secure member of the Wilmington, Delaware Chapter since June 2004.

High Technology Crime Investigation Association - member since August 2002.

High Tech Crime Network - member from September 2001 to date.

National White Collar Crime Center - designated agency contact person for agency membership in the organization - January 2001 to 2009.

Courses Recently Developed

Chip-off / JTAG Bootcamp – A two-day course intended for stand-alone or to supplement a forensic software course. A pilot was recently delivered in January 2017.

Macintosh Digital Forensics – A new course for delivery by Bunting Digital Forensics to various clients. August 2015.

Cyber Security Investigations: Incident Response – New course development and delivery (part of two-person teams) – course was created for virtually delivery using the AvayaLive virtual classroom, with first delivery on June 25, 2014.

Mastering Macintosh Forensics – Rewrite (part of a four-person team) – Alvarez & Marsal for U.S. Department of State ATA – February 2013 – March 2013

Introduction to Digital Forensics and Investigation - Rewrite (part of two-person team) - U.S. Department of State ATA (Humtech) May 2012 - January 2013

Windows Server Incident Response - New course (part of two-person team) - Organization of American States May 2012 - Sept 2012

Advanced Digital Forensics Consultation (Windows / Linux / Macintosh Server Incident Response), New course (solo assignment) plus developed and built portable server lab -U.S. Department of State ATA - Sept 2011 - March 2012

Mastering Macintosh Forensics - New course (solo assignment) - U.S. Department of State ATA - Jan - June 2011

Languages

Primary language is English, however during last several years have spent considerable time teaching and consulting in Latin American countries through interpreters, during which some Spanish skills have been acquired. Currently have the ability and experience demonstrating, teaching, and using EnCase and XRY software using the Spanish interface.

Teaching and Presentation Experience

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, May 9 - 20, 2022, Tirana, Albania (Split - Onsite Delivery / Virtual Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Apr 11 - 22, 2022, Tirana, Albania (Onsite Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Mar 7 - 18, 2022, Tirana, Albania (Onsite Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Jan 10 - 21, 2022, Tirana, Albania (Onsite Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Nov 1 - 19, 2021, Tirana, Albania (Onsite Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Sept 6 - 24, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, May 28 – June 14, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, May 10 - 28, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Apr 5 - 23, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Feb 22 - Mar 12, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Jan11 - 29, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Feb 24 - Mar 13, 2020, Tirana, Albania

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Jan 13 - 24, 2020, Tirana, Albania

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Nov 11 - 22, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Sep 9 - 20, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Jun 20 - Jul 5, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Apr 30 - May 17, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Feb 28 - Mar 22, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Sept 3 – 14, 2018, Beirut, Lebanon.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Aug 6 – 10, 2018, Naperville, IL.

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, July 23 – Aug 3, 2018, Beirut, Lebanon.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – June 18 – 22, 2018, Naperville, IL.

Magnet AXIOM Forensics Course (Online) -Magnet Forensics - Apr. 24-27 2018

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Dec 11-15, 2017, Nigerian MOI in Dubai, UAE.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Nov 27- Dec 1, 2017, Nokesville, VA.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Aug 21-25, 2017, Lansing, MI.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Mar 6-10, 2017, Singapore.

Chip-off Forensics Bootcamp – Sumuri, LLC – January 30, 2017, Dover, DE.

Foundation, Intermediate, XAMN XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 24-28, 2016, Nairobi, Kenya.

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, July 18 - 29, 2016, Shillong, Meghalaya - India.

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – July 6-15, 2016 – Shillong, Meghalaya – India.

Foundation XRY Mobile Phone Forensics – Micro Systemation, A.B. – May 16-17, 2016, U.S. Secret Service National Computer Forensics Institute Hoover, AL.

Foundation and Intermediate XRY Mobile Phone Forensics (private course for 5 members of the Kingdom of Saudi Arabia Ministry of the Interior) – Micro Systemation, A.B. – May 9-13, 2016, London, UK.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Feb 22-26, 2016, Jakarta, Indonesia.

Mobile Device Forensics Consultation, U.S. Department of State ATA, Feb 8-19, 2016, Jakarta, Indonesia.

Foundation & Kiosk XRY Mobile Phone Forensics - Micro Systemation, A.B. – Feb 2-4, 2016 – Singapore

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 21-25, 2015 – Washington, DC

Proactive Internet Investigations Course - U.S. Department of State ATA – Aug 10 - 21, 2015 – Mexico City, Mexico

EnCase Transition Training, Bunting Digital Forensics Custom Course, May 26 – 27, 2015 Delaware State Police Child Predator Task Force, Dover, DE

Foundation and Intermediate XRY Mobile Phone Forensics (private course for 5 members of the Kingdom of Saudi Arabia Ministry of the Interior) – Micro Systemation, A.B. – May 18-22, 2015 – New York, NY

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, May 3 - 14, 2015, Muscat, Oman

EnCase I (Guidance Software Course - ATP) – Abu Dhabi Police Department – Mar 1 – Mar 5, 2015 – Abu Dhabi, United Arab Emirates

Proactive Internet Investigations Course - U.S. Department of State ATA – Jan 26 - Feb 6, 2015 – Cuernavaca, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Jan 16-23, 2015 – Cuernavaca, Mexico

Proactive Internet Investigations Course - U.S. Department of State ATA – Nov 17 - 28, 2014 – Tijuana, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Nov 6-14, 2014 – Tijuana, Mexico

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 20-24, 2014 – Alexandria, VA

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Sep 22-26, 2014 – Santiago, Chile

Proactive Internet Investigations Course – U.S. Department of State ATA – August 11 – 22, 2014 – Ciudad de México, México

Digital Forensic Lab Mentoring and Consulting – Lead Instructor - U.S. Department of State ATA, July 14 – 25, 2014, Medellin & Bucaramanga, Colombia

Cyber Security Investigations: Incident Response – U.S. Department of State FedCTE Program – June 24, 2014, Virtual Class - AvayaLive

Digital Forensic Lab Mentoring and Consulting – Lead Instructor U.S. Department of State ATA, May 5 – 16, 2014, Cali & Pereira, Colombia

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Mar 24 – Apr 4, 2014, Bogota, Colombia

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Apr 7-11, 2014 – Alexandria, VA

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Mar 3-7, 2014 – Vancouver, BC

Proactive Internet Investigations Course - Lead Instructor - U.S. Department of State ATA – Jan 27 – Feb 7, 2014 – Cuidad Juarez, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Jan 20-25, 2014 – Cuidad Juarez, Mexico

Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Nov 20-22, 2013 – San Diego, CA

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Nov 4-9, 2013 – Chihuahua, Mexico

Computer Forensics for Legal Professionals, September 24, 2013, Widener University School of Law, Wilmington, DE

Introduction to Digital Forensics and Investigation - Lead Instructor - U.S. Department of State ATA, September 2-13, 2013, Mexico City, Mexico

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, July 15-26, 2013, Dakar, Senegal

Introduction to Digital Forensics and Investigation (New Version Pilot) - Lead Instructor - U.S. Department of State ATA, April 8-19, 2013, Manila, Philippines

Identification & Seizure of Digital Evidence - Lead Instructor - U.S. Department of State ATA – Mar 9-17, 2013 – Muscat, Oman

Identification & Seizure of Digital Evidence - U.S. Department of State ATA - Feb 11-21, 2013 - Dakar, Senegal

Mastering Macintosh Forensics, Alvarez & Marsal, Oct 29 - Nov 2, 2012, 2012, Washington, DC

Incident Response Tabletop Exercise, large web hosting client, Oct 16-17, 2012, San Antonio, TX

Macintosh Incident Response, HTCIA, Sept 16-19, 2012, Hershey, PA

Windows Server Incident Response - Lead Instructor - Organization of American States, Sept 3-7, 2012, Trinidad & Tobago

Fundamentals of Network Security, U.S. Department of State ATA, July 23 - Aug 3, 2012, Bogota, Colombia

Introduction to Digital Forensics and Investigation (Pilot for revised program) - U.S. Department of State ATA, April 23 - May 4, 2012, Mexico City, Mexico

Mastering Macintosh Forensics, Ocean County Prosecutor's Office, April 16-20, 2012, Tom's River, NJ

Advanced Digital Forensics Consultation (Windows / Linux / Macintosh Server Incident Response), Developer and Lead Instructor - U.S. Department of State ATA Mar 5-16, 2012, Bogota, Colombia

Cyber Unit Management Consultation, U.S. Department of State ATA, Sept 5-16, 2011, Bogota, Colombia

Cell Phone Forensics Consultation, U.S. Department of State ATA, July 11-22, 2011, Antigua.

Macintosh Forensics & Advanced Forensics Consultation, Developer and Lead Instructor - U.S. Department of State ATA, June 6-17, 2011, Bogota, Colombia.

Forensic Equipment Grant Consultation, U.S. Department of State ATA, May 17-31, 2011, Bangkok, Thailand

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, May 2-13, 2011, Mauritius

Advanced Forensic Acquisition & Analysis - Delaware ICAC - March 21-25, 2011, Dover, DE

Forensic Acquisition & Analysis - Delaware ICAC- Feb 21-25, 2011, Dover, DE

Cyberbullying - Cape Henlopen High School - January 27, 2011, Lewes, DE

Software Consultation: EnCase 1 & EnCase 2, U.S. Department of State ATA, Jan 10-21, 2011, Bangkok, Thailand

Incident Response & Forensic Tools Overview - Delaware Cyber Terrorism Exercise, Oct 27, 2010, Smyrna, DE

Identification & Seizure of Digital Evidence - U.S. Department of State ATA - June 3 - 11, 2010 - Mexico City, MX

EnCase Computer Forensics I – Lead Instructor - North Carolina ICAC- April 26 - 30, 2010 - Raleigh - Durham, NC

EnCase Computer Forensics II – Lead Instructor - Sidley Austin LLP - February 22 - 25, 2010 - Chicago, IL

EnCase Computer Forensics I - Qatar National Bank - October 11 - 15, 2009 - Doha, Qatar

EnCase Computer Forensics I - Abu Dhabi Police Department - October 4 - 8, 2009 - Abu Dhabi, UAE

Introduction to Computer Forensics - University of Delaware Police - August 17-21, 2009 - Lewes, DE

Advanced Computer Forensics Techniques - Computer Forensics Analysis and Training Center - June 4-5, 2009 - Sharon Hill, PA.

Cyberbullying - May 11, 2009 - Long Neck Elementary School - Millsboro, DE

"Computer Forensics - Current State and Future Challenges" - Computer Crimes Colloquium - April 7, 2009 - Wilmington University - Dover, DE

Identity Theft - City of Lewes Neighborhood Watch Meeting - March 23, 2009 - Lewes, DE

Disaster Recovery (CIS 486) - Goldey-Beacom College - January to March 2008 - Wilmington, DE.

Forensic Acquisition and Analysis - November 16-20, 2008, Dubai Police Department, Dubai, UAE

Cyber Stalking - Delaware Domestic Violence Council - Dover Police Department, November 7, 2008, Dover, DE

Computer Forensics (CIS 362) - Goldey-Beacom College - October to December 2008 - Wilmington, DE.

Advanced Computer Forensics - September 22-26, 2008, Sidley - Austin in Chicago, IL

Computer Forensics Primer for the Press - September 17, 2008 - Delaware Valley Press Club - Chester, PA.

Investigation Crimes Involving Computers - August 28-29, 2008 - Newark, DE.

Introduction to Computer Forensics - Computer Forensics and Analysis Training Center - August 26-27, 2008 - Sharon Hill, PA.

Disaster Recovery (CIS 486) - Goldey-Beacom College - March to April 2008 - Wilmington, DE.

Computer Forensics (CIS 362) - Goldey-Beacom College - October to December 2007 - Wilmington, DE.

Computer Forensics for Medical / Legal Professionals - University of Delaware Special Programs - November 9, 2007

Windows Network Investigations and Forensics - HTCIA Regional Training - June 19, 2007 - Newark, DE

User Services - First Response to Crime Scenes Workshop - Special Interest Group on University and College Computing Services - Edmonton, Canada - November 5, 2006

Cyber Stalking - Delaware Domestic Violence Council - November 16, 2006 - Dover, DE.

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 28, 2006 - Dewey Beach, DE.

CyberSpeak Podcast - Microsoft Log Parser Forensic Applications - June 3, 2006

CyberSpeak Podcast - User Assist Registry Key and Restore Point Forensics - May 13, 2006

Investigation of Cyber Incidents - University of Delaware System Administrators Group - May 17, 2006 - Newark, DE

Identity Theft and Cyber Safety - DuPont Experimental Station Staff - March 14, 2006 - Wilmington, DE.

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 22, 2005 - Lewes, DE.

First Response Issues for Crimes Involving Computers - Hosted by the U.S. Attorney's Office - September 16, 2005 - Dover, DE.

Examination of Photoshop Layer Data - RCFG GMU 2005 - August 15 & 18, 2005 - Fairfax, VA

Cyber-sabotage, Espionage, & Other Security Threats, February 23, 2005, Lorman Education Services, Newark, DE

Computer Forensics in the Courtroom, January 7, 2005, Widener University School of Law, Wilmington, DE

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 30 - October 1, 2004 - Dewey Beach, DE.

Forensic Examination of Peer-to-Peer Client Software Artifacts -NJSP High Tech Crime Unit. September 22, 2004, Trenton, NJ.

Introductory Computer Forensics Guidance Software - Sterling, VA Jun 29 - Jul 2, 2004 (32 hrs) Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Jun 22 - 25, 2004 (32 hrs) Lead Instructor

Email Examinations Lab at CEIC 2004 Myrtle Beach, SC Jun 6 - 9, 2004 (7.5 hrs - five presentations) Lead Instructor

Photoshop Layer Metadata Examinations CEIC 2004 Myrtle Beach, SC Jun 8, 2004 (1.5 hrs) Lead Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Apr 27 - 30, 2004 (32 hrs) Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Mar 30 - Apr 2, 2004 (32 hrs) Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Feb 3-6, 2004 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Jan 6-9, 2004 (32 hrs) Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Nov 18-21, 2003 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Oct 21-24, 2003 (32 hrs) Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA Sept 9-12, 2003 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Aug 12-15, 2003 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA July 8-11, 2003 (32 hrs) Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA June 17-20, 2003 (32 hrs) Instructor

Internet / Email Guidance Software - Sterling, VA May 6-9, 2003 (32 hrs) Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA Mar 4-7, 2003 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Feb 25-28, 2003 (32 hrs) Instructor

Internet Safety for Children - Winter / Spring 2003 semester offering through the University of Delaware Continuing Education Division

Cyber-Stalking and Related Crimes Involving Computers: October 7, 2002 in Newark, DE.

Computer Crime Issues for Prosecutors: - Presented to the Wicomico County States Attorney's Office (4/20/01) and to the Attorney General's Office for the State of Delaware Sex Crimes Unit (10/4/02).

Computer Forensics: - during the spring semester 2002, supervised and directed an independent course of study in computer forensics for a University of Delaware senior majoring in computer science. Program was under the auspices of Professor Chien-Chung Shen. Student is now employed with Price, Waterhouse, Cooper in the computer forensics division.

The Internet as an Investigative Tool: Presented at the University of Delaware (5 presentations: 12/5/00, 1/8/01, 8/6/01, 8/13/01, & 8/26-27/02), at the Eastern Shore Criminal Justice Academy (3 presentations: 2/16/01, 3/8/01, and 3/20/01), and at Mount St. Mary's College (6/26/02).

Computer Crimes: 1st Responder Issues - course developed and presented to the University of Delaware Police as a 2-hour block during in-service training. Presented May 31, 2001, June 7, 2001, May 30, 2002, and June 5, 2002.

Training Courses Completed

Counterterrorism Assistance Planning Event	U.S. Dept of State – Oct 19 – Nov 4, 2022 Virtual
Magnet Forensics Virtual Summit 2020	Magnet Forensics – May 4 – 29, 2020 Virtual
XRY Train-the-Trainer Training	MSAB – Aug 19– 23, 2019 Stockholm, SE
X1 Social Discovery	Digital Shield – April 9-11, 2019 Online
XRY Train-the-Trainer Training	MSAB – Aug 23–26, 2018 Washington, DE
HTCIA Conference	HTCIA – Aug 19-22, 2018 Washington, DC
AX300 – AXIOM Advanced Mobile Examinations	Magnet Forensics – Oct 24-27, 2017 Sterling, VA
iVE Vehicle Forensics	Berla – Sep 25-29, 2017 Annapolis, MD
AX200 - AXIOM Examinations	Magnet Forensics – Sep 19-22, 2017 Online
XRY Train-the-Trainer Training	MSAB – Aug 30– Sep 1, 2017 Stockholm, SE
XRY Version 7 Training	MSAB – Aug 22–26, 2016 Stockholm, Sweden
XRY Version 7 Training	MSAB – Mar 28–Apr 1, 2016 Stockholm, Sweden
XRY Advanced Acquisitions	MSAB – Mar 21 – 25, 2016 Freehold, NJ
XRY Advanced Applications Analysis	MSAB – Dec 14 – 18, 2015 Washington, DC

XRY Train-the-Trainer Annual Training	MSAB – Sept 7-11, 2015 Stockholm, Sweden
XRY Train-the-Trainer Course	MSAB – Sept 30- Oct 11, 2013 Stockholm, Sweden
FTK Bootcamp Version 3	Access Data - April 5-7, 2011 - Online
XRY Physical Acquisition & Analysis Training	MSAB - Oct 6-8, 2010 - Alexandria, VA
XRY Logical Acquisition & Analysis Training	MSAB - Oct 4-5, 2010 - Alexandria, VA
Basic Malware Analysis	HB Gary - April 20-21, 2010 - Columbia, MD
LAW PreDiscovery Certified Administrator Course	LexisNexis - Jan 14, 2010 - Washington, D.C.
LAW PreDiscovery EDD Certified User Course	LexisNexis - Jan 12-13, 2010 - Washington, D.C
Microsoft Exchange Server 2007	Global Knowledge - Jan 26 - 30, 2009 - Arlington, VA
HTCIA Conference (24 hrs)	High Tech Crime Investigator's Association - Oct 20-22, 2008, Atlantic City, NJ
Operation Fair Play (40 hrs)	Delaware State Police ICAC – Wyoming Tool Kit Training - Mar 31-Apr 4, 2008, Dover, DE
Neutrino Cell Phone Forensics (16 hrs)	Guidance Software - January 15 – 16, 2008, Sterling, VA.
Macintosh Forensics (40 hrs)	Phoenix Data Group - October 15-19, 2007 - Sharon Hill, PA
Vista Forensics	Access Data - July 20, 2007 - Washington, DC
Advanced Windows Intrusion Investigator's Course (40 hrs)	SYTEX - February 27 – March 3, 2006, FBI Academy, Quantico, VA
Adobe Photoshop for Forensic Video Analysts (16 hrs)	Resolution Video - December 14-15, 2005 - Reston, VA
Regional Computer Forensics Group Seminar (40 hrs)	RCFG / HTCIA - August 15-19, 2005 - GMU - Fairfax, VA.
Cell Seizure (16 hrs)	Paraben - May 18-19, 2005 in Newark, DE
PDA Seizure (16 hrs)	Paraben - May 16-17, 2005 in Newark, DE

Enterprise Security & Vulnerability (36 hrs)	USSS / SEARCH - April 18-22, 2005 in Cherry Hill, NJ
Access Data FTK Advanced Internet Training Course (24 hrs)	Access Data - March 15 – 17, 2005 in Dover, DE.
Ocean Systems: dTective (Advanced Video Forensic Analysis) (16 hrs)	Ocean Systems - Feb. 24 – 25, 2005 in Burtonsville, MD.
Advanced UNIX Investigator's Course (40 hrs)	SYTEX - December 6 – 10, 2004, Ellicott City, MD.
EnCase EnScript Programming (32 hrs)	Guidance Software - November 16 – 19, 2004, Sterling, VA.
Networks and Networking for Agents / System Security and Exploitation (80 hrs)	SYTEX - October 18 – 29, 2004, Ellicott City, MD.
Law Enforcement Video Association Annual Training Conference 2004 (16 hrs)	LEVA - October 6 – 7, 2004 Washington, D.C.
NIJ Law Enforcement Technology Institute 2004 (40 hrs)	NIJ - July 11 – 16, 2004, Washington, D.C.
Computer and Enterprise Investigations Conference / TechnoSecurity Conference 2004 (28 hrs)	Guidance Software - June 6 – 9, 2004 in Myrtle Beach, SC.
Ocean Systems: dTective (Advanced Video Forensic Analysis) (16 hrs)	Ocean Systems - May 6 – 7, 2004 in Burtonsville, MD.
Ocean Systems: Introduction to Forensic Video Examinations (24 hrs)	Ocean Systems - May 3 – 5, 2004 in Burtonsville, MD.
Access Data FTK Intermediate Training Course (24 hrs)	Access Data - April 5 – 7, 2004 in Dover, DE.
EnCase Expert Series: Internet & Email Examinations (32 hrs)	Guidance Software - February 4 - 7, 2003 in Sterling, VA.
EnCase Advanced Computer Forensics (32 hrs)	Guidance Software - January 21- 24, 2002 in Sterling, VA.
Introduction to Programming Concepts (Visual Basic 6) (50 hrs)	University of Delaware Course - Wilm, DE – Fall 2002
Computer and Enterprise Investigations Conference 2002 (16 hrs)	Guidance Software - September 16-17, 2002 Chantilly, VA.

Regional Computer Forensics Group Seminar (40 hrs)	RCFG / HTCIA - August 12-16, 2002 - GMU - Fairfax, VA.
ILook Computer Forensics Software (24 hrs)	ACES / FBI / IRS / NCFS - July 23-25, 2002 Orlando, FL.
Firewalls and Virtual Private Networks (16 hrs)	CSI / NIPC / FBI - May 22-23, 2002 MSP - Columbia, MD.
Internet Investigations and Child Exploitation Overview (8 hrs)	SEARCH - April 6, 2002, CCU - Conway, SC.
Techno-Security 2002 Conference (28 hrs)	The Training Company - April 7-10, 2002 - Myrtle Beach, SC
Enterprise Networks (50 hrs)	University of Delaware - Wilm, DE - Spring 2002
EnCase Advanced Computer Forensics (32 hrs)	Guidance Software - February 19-22, 2002 - Leesburg, VA.
LAN (Local Area Networks) (50 hrs)	University of Delaware - Newark, DE - Fall 2001
EnCase Intermediate Computer Forensics (32 hrs)	Guidance Software - August 7-10, 2001 - Leesburg, VA .
Techno-Security 2001 Conference (28 hrs)	The Training Company April 22-25, 2001 - Myrtle Beach, SC
WAN (Wide Area Networks) (50 hrs)	University of Delaware - Newark, DE - Spring 2001
Advanced Data Recovery and Analysis Course (40 hrs)	NW3C - October 23-27, 2000 - Fairmont, WV.
The Internet as in Investigative Tool (8 hrs)	NW3C / IFCC - October 12, 2000 - Fairmont, WV.
Basic Data Recovery and Analysis Course (40 hrs)	NW3C July 24-28, 2000 in Myrtle Beach, SC.

Computer Forensics Expert Witness Experience

STRIKE 3 HOLDINGS, LLC v. JOHN DOE SUBSCRIBER ASSIGNED IP ADDRESS 68.83.56.212 and STRIKE 3 HOLDINGS, LLC v. JOHN DOE INFRINGER INDENTIFIED AS USING IP ADDRESS 69.113.113.228 – U.S. District Court of New Jersey in Camden – Testified at two hearings, May 31, 2019 and July 23, 2019, regarding the function of peer-to-peer bittorrent software, detecting

copyright infringers, and basics of networking and IP addresses on behalf of the plaintiff alleging copyright infringement using bittorrent software to download protected works.

Deposed on April 10, 2019 in Georgetown, DE in the matter of LendUS, LLC vs John Goede & John Schrenkel (C.A. No. 2018-0233-SG), on behalf of the plaintiff. Defendant claims text messages on his phone were deleted when plaintiff caused Verizon to suspend his telephone service and thus the plaintiff's actions precluded the defendant from complying with discovery request to produce said messages. Testified and demonstrated that cutting off from service does not delete messages, as messages are stored on the iPhone proper.

Laser Tone Business Systems, LLC vs Delaware Micro-Computer, PrintIT Solutions, Alex J. Farling, and Justin McGinnis (CA No. 2017-0429-TMR). On behalf of plaintiff, conducted a forensic examination of computers used by McGinnis and documented evidence that showed exfiltration of IP data. The exfiltrated data was used to jump start a competing business. The initial report served as a basis to shut down the competing business and bring about a settlement. McGinnis did not settle and the matter went to trial, during which Mr. Bunting testified at deposition (August 15, 2018) and later at trial (December 6, 2019) concerning the forensics findings. As of 4/13/19, the judge has not yet rendered a decision in the case.

Crawford and Company v Larry W. Daniel and Cunningham Lindsey Claims Management, Inc Civil Case No 17-1-01244 – Superior Court of Cobb County State of Georgia – Submitted affidavit on September 12, 2017 on behalf of Crawford that an iPhone submitted by the defendant as part of electronic discovery had the messages set to delete after 30 days and that the user has enabled backup encryption, thereby preventing the contents from being acquired. Case settled without going to trial.

AdMarketer, LLC and Credit Benefit Services, LLC v Isaac "Zack" Bernato; Dennis H. James; CRM Holding Company, LLC; IMT Marketplace, LLC; World Clicks, LLC; and Valerie DiNardo – Civil Action File No: 2015CV267337 in the Superior Court of Fulton County State of Georgia – Submitted affidavit on March 31, 2017 on behalf of the defendant that opposing expert had made a finding that defendant had deleted messages, thus supporting a spoliation claim. Affidavit stated that opposing expert had not discovered iPhone message setting for 'delete after 30 days' nor had he discovered that SMS forwarding was enabled, enabled specifically to a Mac laptop that was in the possession of the opposing expert and which opposing expert had failed to examine. This laptop contained all the chat messages that the expert claimed were deleted. Further the affidavit stated that the opposing expert had used only one tool in his examination and in doing so missed over 11,000 AIM messages, many of which were relevant to the case. Defendants filed bankruptcy and case settled without trial.

Tamika Covington vs International Association of Approved Basketball Officials, Board 193, et al. (CIVIL ACTION NO. 3:08-cv-03639) - US District Court (Princeton, NJ) – Testified as expert for defense in computer forensics analysis and email analysis in a hearing to dismiss based on fraudulent documents offered into evidence by plaintiff. Specifically, testified that document proffered as an email was in fact fabricated to appear as such. – July 09, 2014.

Network Computing Services Corporation vs Haynsworth, Sinkler, P.A. Belton T. Zeigler and John Tiller (South Carolina) – Submitted two affidavits for the plaintiff regarding deleted emails in a case alleging legal malpractice – April 2010

State of Delaware vs Irina Malinovskaya (3rd trial - Murder 1st) – Testified as computer forensics expert regarding analysis of defendant's computer. Also testified that an email offered by the defendant after the 2nd trial was fabricated and offered as evidence. The defendant was convicted of tampering with physical evidence. - 2007

Cpl B. Kurt Price et al. vs Colonel L. Aaron Chaffinch et al. (US District Court) Submitted affidavit as to wiping of a hard drive by the plaintiff - May 2006

State of Delaware vs Irina Malinovskaya (2nd trial - Murder 1st) Testified - 2006

State of Delaware vs Stephanie McMullen (Munchausen's Nurse case) Testified - 2006

State of Delaware vs Eric Kemske (Manufacture, distribute, possess child pornography – peer-to-peer software involved) – Testified - 2005

State of Delaware vs Keith Appleby (Suppression Hearing - Computer Intrusion Case) Testified - 2003

EXHIBIT A-8

Affidavit of Stephen Michael Bunting

State of Delaware
County of Sussex

COMES NOW Stephen Michael Bunting, being first duly sworn, under oath, and states that the contents of the following attached reports, including their appendices, and exhibits are true and correct statements of relevant facts and his opinions in the case of United States v. Keith Raniere et. al., in the United States District Court, Eastern District of New York, Case #: 1:180-cr-00204-NGG-VMS, to the best of his knowledge and belief:

- Forensic Review of Dr. J. Richard Kiper's Technical Findings in the matter of U.S. v. Raniere, et al., 18 CR 204 (NGG) with three appendices

Signature: _____

Address: 33579 Blue Heron Drive
Lewes, DE 19958

SUBSCRIBED AND SWORN TO before me this 22 day of September, 2022, by Stephen Michael Bunting.

VICTORIA KOPUNEK
MY COMMISSION EXPIRES
NOTARY
PUBLIC
JULY 12, 2023
STATE OF DELAWARE

Victoria Kop
NOTARY PUBLIC FOR DELAWARE

My Commission Expires: 07/12/2023

Stephen M. Bunting
Senior Forensic Consultant / CEO Bunting Digital Forensics, LLC
2022 Sept 21

Forensic Review of Dr. J. Richard Kiper's Technical Findings

RE: Matter of U.S. v. Raniere, et al., 18 CR 204 (NGG)

Professional Background:

I served as a Captain with the University of Delaware Police from 1980 to 2009, with the last ten years of that career in digital forensics and cyber investigations. I created the digital forensics unit from its inception and ran it until my retirement in 2009. I conducted hundreds of forensic examinations for numerous agencies. I was a part-time instructor during that time, 2003-2004, for Guidance Software, the makers of EnCase forensic software. I've trained hundreds of forensic examiners from federal, state, and local law enforcement agencies as well as private agencies and international police.

Since retirement in 2009, I worked for Forward Discovery, which was bought out by Alvarez and Marsal. In 2013 I left Alvarez and Marsal and formed my own practice, Bunting Digital Forensics, LLC. Since 2009 my private sector duties have included forensic examinations in Medicaid fraud, intellectual property theft, email forgery, copyright infringement over peer-to-peer networks, spoliation, telecommunications fraud, malware, mobile device forensics, eDiscovery collections, Macintosh examinations, and limited criminal defense casework. Since 2013 I have been a contract instructor for MSAB in Sweden, makers of XRY / XAMN mobile device forensic software, teaching classes in the U.S. and internationally.

Since 2008 I have been a contract instructor for the U.S. Dept of State Antiterrorism Assistance Program (ATA) Cyber Division. During my 15 years with ATA I have taught, as lead instructor, nearly all their cyber course offerings in well over twenty countries. I have been a mentor for ATA as well. Currently I am an embedded mentor for the Albania State Police Counter Terrorism Directorate and their Computer Audio Video Forensics Unit, having done so since 2019 and have been in country over a dozen times. One of my projects there is creating a new digital forensics lab at their Counter Terrorism Directorate.

I have received numerous certifications over the years in computer forensics, mobile forensics, and vehicle forensics. I have testified in federal and state courts and have been recognized as an expert in computer forensics at both levels. I have assisted in various phases of establishing accredited laboratories, including pre-assessment / planning, training, policy and procedure development, and mentoring. I've written five textbooks in the field and published numerous

articles. I have an in-depth knowledge of a broad range of digital forensics as well as policies and procedures on which digital laboratory accreditation is based.

Review of Evidence:

On September 10, 2022, I signed the Protective Order Regarding Discovery in U.S. v. Raniere, et al., 18 CR 204 (NGG) and was subsequently provided access to certain evidence in this case. My review of evidence includes court testimony, a "drag-and-drop" copy of selected files from a WD HDD, and examination reports generated by members of the FBI's Computer Analysis Response Team (CART). In addition, I have read Dr. Kiper's affidavits containing his technical findings, the attached reports, and his analysis of SA Flatley and SA Booth testimonies.

Dr. Kiper has concluded in his affidavits and reports that he "discovered specific actions that were taken to manually alter the evidence, in support of the government's narrative that photos were taken by a Canon EOS 20D camera (GX 520), saved to a Lexar CF card (GX 524), copied to an unknown computer, and then backed up to a Western Digital hard disk drive (GX 530)." Dr. Kiper refers to the latter two items as the CF Card and the WD HDD. I will do likewise.

I have reviewed Dr. Kiper's findings and have made the same observations in the data as did he. I verify and confirm his findings regarding the data. Further, I concur with his conclusions that multiple and intentional alterations to the digital evidence occurred that would constitute evidence manipulation. To a scientific certainty, data alterations took place while the evidence was in the custody of the FBI, specifically while the CF Card was signed out to SA Lever, the special agent in charge of the investigation. There are many alterations to the data that all lean in the direction of the government's narrative. I concur with Dr. Kiper's expert opinion that the FBI had to have been involved in evidence tampering in this matter.

Review of Kiper's Key Technical Findings:

Finding 1. Some digital photo files found on the CF card had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people. Moreover, these same CF card files contained thumbnail pictures from another existing set of photos, thus proving manual alteration of the CF Card contents.

To verify this finding, I observed that the modified dates of the files IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG, and IMG_0097.JPG had the same exact dates on both the CF Card and the WD HDD. Respectively, the modification dates for those files was 10/19/2005 7:33 PM at 18, 26, 52, and 58 seconds. The information was obtained from GX 521A_Replacement.pdf and GX 505A.pdf. The former was the FBI CART generated report for the CF Card, while the later was for the WD HDD.

On the CF Card, there is no viewable content for these four files (IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG, and IMG_0097.JPG), yet on the WD HDD, the files are viewable. One would expect that if these four files on the WD HDD were backup copies of those same named four files on the CF Card, they would display the same content, especially as they had the same exact modification timestamps, but such is not the case. The thumbnails were carved from each set of the four files from the CF Card and the WD HDD and they were hashed, using an MD5 hash. Visually, the thumbnails from the CF Card did not match their same named counterparts on the WD HDD. They were vastly different when they should have been the same. Consistent with visual observation, the hashes did not match.

The thumbnail hashes of these four files on the CF Card (IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG, and IMG_0097.JPG) did however match the thumbnail hashes of four files found on both the CF Card and the WD HDD. Those files were IMG_180-3 (.JPG). Thus the data for the four files on the CF card (IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG, and IMG_0097.JPG) originated from the files IMG_180-3 (.JPG). As the four files (IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG, and IMG_0097.JPG) on the WD HDD were supposed to have been backups of their named counterparts on the CF Card, they are in fact not. They are different when they should have been identical.

There is no normal operation of the camera and backup process that would produce two sets of files, named the same, last modification times the same, and should be the same content, but yet are not be the same.

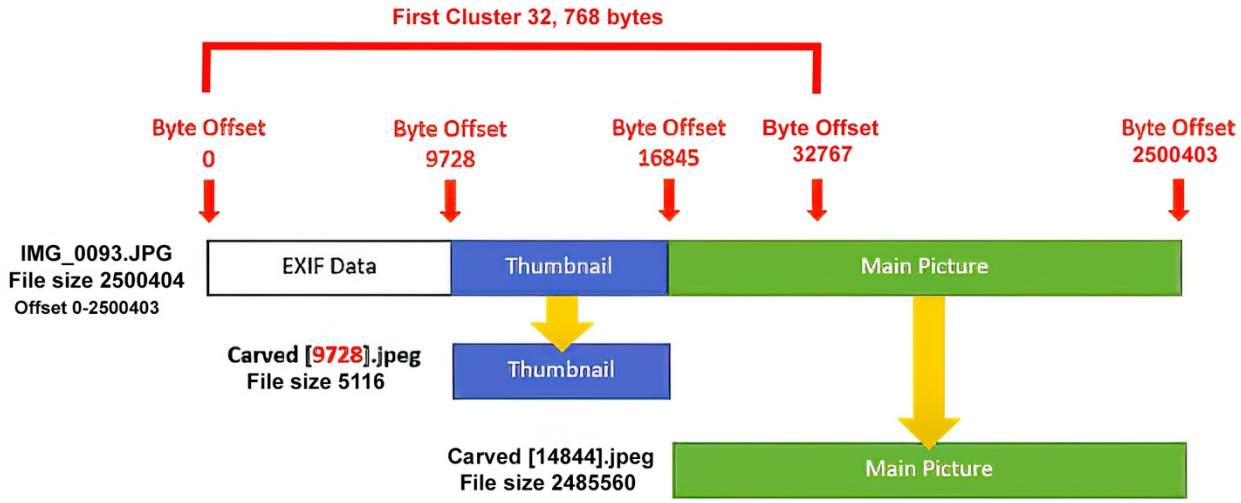
The Canon 20D defaults to continuous numbering so duplicate numbers are unlikely, especially with same exact timestamps. To create this condition “in camera”, one would have had to create original set of pictures and place them elsewhere, format the card, turn off continuous numbering, manually roll back camera to previous time, and carefully match taking a second set of photos so as to match the time down to the second. This is a possibility at the most extreme, yet incredibly difficult to achieve and very unlikely. The simplest answer, though, given the accessed times that occurred while in FBI custody is manual manipulation.

Oddly enough, the FBI was not able to start the camera as the battery was dead due to the length of time that the camera had sat idle. Rather than procure a replacement battery for $10 to $12, the camera’s settings were never examined and recovered. We don’t know the numbering settings nor the accuracy of the time that created the original EXIF timestamps, upon which much of the government’s evidence was based. Most modern Canon cameras use a super capacitor to retain time and settings when the battery is removed. Whether this capacitor still held a charge and thus would have enabled the FBI to have queried the time accuracy and settings was never pursued, despite the import of the accuracy of photo dates and times to the government’s case. The date and time on the 20D is manually entered and does not come from GPS satellites as is the case on many cameras or from network time with smart phones. Normally, when a device (computer, camera, mobile device, etc.) is seized, one of the first things that is done is to check the device time with a known time standard. This helps establish the accuracy or inaccuracy of the device creating the timestamps in the EXIF

metadata and the original file system metadata on the camera's media card, the CF Card in this case. This was never done despite the import of the timestamps to the government's case.

The four photos (IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG, and IMG_0097.JPG) on the CF Card are recovered deleted files. On the CF Card version of the files, they have prefix of ! (exclamation mark) instead of an I (capital letter i). This naming convention occurs because, during the file deletion process, the first character of the file name is changed to the hex value E5 to denote its deleted status in the FAT Directory Entry. During the recovery process, since the value of the first letter of the file name is no longer known (replaced by hex E5), it is represented by the character ! in the forensic software. As nearly all files begin the prefix IMG on the CF Card, we know this ! used to be an I before it was deleted.

Thus, these four files (IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG, and IMG_0097.JPG) were recovered via their FAT Directory entries. It is possible to have fragmented clusters and the clusters beyond the starting cluster could have come from another file during the deleted file recovery process, BUT the cluster size for a 2 GB FAT 16 created by the Canon 20D is 32,768 bytes. So the starting cluster, firmly defined in the FAT entry, would have included the entire thumbnail. The thumbnail would NOT be impacted and thus cluster run errors due to fragmentation would not be a viable explanation for the thumbnails not matching. The diagram below shows this point quite explicitly. The simplest and only plausible answer, though, given the accessed times that occurred while in FBI custody and all the other anomalies is manual manipulation.



This diagram is from Dr. Kiper's Report in Appendix C where he shows how carving works. This diagram has been changed to show the data for IMG_0093.JPG and overlays the first or starting cluster onto that diagram. The starting cluster is defined in the FAT Directory Entry and fully includes the EXIF data, the entire thumbnail, and the beginning of the main picture. Any erroneously assigned clusters would occur AFTER the starting cluster and thus would NOT be a valid explanation for why the thumbnails do not match their named counterparts on the WD HDD, neither visually or by their hash values.

Finding 2. Additional files appeared on the FBI's forensic report of the CF Card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the CF Card and the WD HDD.

I reviewed a report created by FBI CART Examiner Stephen Flatley, using Forensic Toolkit, which was created on 4/11/19 and lists all active files present on the CF Card as well as those that have been deleted.

I also recognize that this report appears to only contain the photo files for the CF Card, as files that I would expect to be present, non-photo files and folders, are not present. For example, I just used the exact same model CF card as was used in the case (Lexar 2GB), formatted it in the camera, using the same exact make / model camera (Canon 20D), and took pictures. I immediately imaged the card using a write blocker before the card has ever been mounted on a computer. Using FTK Imager to create the image, one of the options is to automatically create a file and directory listing of all objects on the device. I chose that option and thus the CSV report was automatically generated. There are files that are at the top and bottom of this list that I would have expected to find in Flatley's report, so it is clear that the report has been reduced to only include photo files. The files I would expect to find and did not are shown in the following to screen captures.

Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Del
[root]	Partition 1\EOS_DIGITAL [FAT16]\[root]\	16384				no
VBR	Partition 1\EOS_DIGITAL [FAT16]\VBR	512				no
[unallocated space]	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\	0				no
file system slack	Partition 1\EOS_DIGITAL [FAT16]\file system slack	24576				no
FAT1	Partition 1\EOS_DIGITAL [FAT16]\FAT1	124928				no
FAT2	Partition 1\EOS_DIGITAL [FAT16]\FAT2	124928				no
DCIM	Partition 1\EOS_DIGITAL [FAT16]\[root]\DCIM\	32768	2022-Sep-15 02:47:22	2022-Sep-15 02:47:22		no
System Volume Information	Partition 1\EOS_DIGITAL [FAT16]\[root]\System Volume Inform	32768	2022-Sep-15 14:46:25.2	2022-Sep-15 14:46:26		no
135CANON	Partition 1\EOS_DIGITAL [FAT16]\[root]\DCIM\135CANON\	32768	2022-Sep-15 02:47:22	2022-Sep-15 02:47:22		no
136CANON	Partition 1\EOS_DIGITAL [FAT16]\[root]\DCIM\136CANON\	32768	2022-Sep-15 03:10:52	2022-Sep-15 03:10:52		no
IMG_3543.JPG	Partition 1\EOS_DIGITAL [FAT16]\[root]\DCIM\135CANON\IMG_	2903452	2022-Sep-15 02:56:40	2022-Sep-15 02:56:40		no

Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Deleted
IMG_3603.JPG	Partition 1\EOS_DIGITAL [FAT16]\[root]\DCIM\136CANON\IMG_	1849401	2022-Sep-15 03:10:54	2022-Sep-15 03:10:54		no
WPSettings.dat	Partition 1\EOS_DIGITAL [FAT16]\[root]\System Volume Inform	12	2022-Sep-15 14:46:25.2	2022-Sep-15 14:46:26		no
IndexerVolumeGuid	Partition 1\EOS_DIGITAL [FAT16]\[root]\System Volume Inform	76	2022-Sep-15 14:46:25.4	2022-Sep-15 14:46:26		no
7	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\00007	104857600				no
3207	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\03207	104857600				no
6407	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\06407	11239424				no
8947	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\08947	2457600				no
9245	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\09245	3899392				no
13398	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\13398	104857600				no
16598	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\16598	104857600				no
19798	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\19798	104857600				no
22998	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\22998	104857600				no
26198	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\26198	104857600				no
29398	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\29398	104857600				no
32598	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\32598	104857600				no
35798	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\35798	104857600				no
38998	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\38998	104857600				no
42198	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\42198	104857600				no
45398	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\45398	104857600				no
48598	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\48598	104857600				no
51798	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\51798	104857600				no
54998	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\54998	104857600				no
58198	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\58198	104857600				no
61398	Partition 1\EOS_DIGITAL [FAT16]\[unallocated space]\61398	27721728				no
MBR	Unpartitioned Space [basic disk]\MBR	512				no
[unallocated space]	Unpartitioned Space [basic disk]\[unallocated space]\	0				no
1	Unpartitioned Space [basic disk]\[unallocated space]\0000001	31744				no
3984120	Unpartitioned Space [basic disk]\[unallocated space]\3984120	12644352				no

I reviewed a report created by FBI CART Examiner Brian Booth, using ForensicToolkit, which was created on 6/11/19 and lists all active files present on the CF Card as well as those that have been deleted. It is worthy to note, as did Dr. Kiper, that creating another forensic image and another report is not only unusual, but against FBI Policy, requiring high level authorization. The authorization in this case was given by SSA Schmatz, and not by someone with the level of permission required under policy. Nevertheless, one would expect that the same process (imaging) applied to the same data source (CF Card) would provide the same exact result. It is supposed to. During the imaging process, the source CF Card, and the resultant image are hashed often by two hashing algorithms. When done, the image is hashed and compared to the acquisition image hash. They should match. If they don't, there's a problem and reason must be investigated and resolved. This process was done twice, once by Flatley and once by Booth. Both should have been verified upon completion and the hash of the second image by Booth should have been compared to the one by Flatley to ensure they matched, especially due to the unusual process of imaging twice the same CF card. There is no indication or record of this having been done.

The report created by Booth also lacked the same non-photo files shown in the above two screenshots and only included photo files. When the Booth report was compared to the Flatley report, there was a discrepancy in the total numbers of files between the two reports, i.e Flatley reported 43 photo files and Booth reported 80 photo files. Said another way, the Booth report, GX 521A_Replacement.pdf, has added 37 more files to the case than in the original report by Flatley. Specifically, those file names added were: IMG_0042, IMG_0081–IMG_0100, IMG_0172–IMG_0179, and IMG_0193–IMG_200, all with JPG extensions.

The Booth report was generated on 6/11/19, with Booth testifying to said report beginning on 06/12/19. The reason given for not using Flatley's report is that he was suddenly given an assignment in Africa before he was due to testify. It is important to note that Flatley had given previous testimony stating that metadata could be easily altered and could not be considered reliable by itself. The government's case in this matter rested heavily on EXIF data and Booth would eventually testify that EXIF data is very reliable, the complete opposite of what Flatley had previously said in sworn testimony.

Having imaged thousands of devices in an over twenty-three year career in the field of digital forensics, how two different examiners using the same software (AccessData FTK Toolkit V 6.3.1.26) could image the same source (CF Card), which is supposed to be preserved as seized, unaltered in any way, and arrive at two different sets of data is hard to reconcile.

In examining those addition files, as Dr. Kiper noted, there are reasons to suspect the newly appearing files did not originate from the CF Card, but rather were manually added (planted).

1) I note, as did Dr. Kiper, that none of the files for the filenames added to the 6/11/19 report can be viewed. By contrast all the files that appeared in the 4/11/19 report can be viewed.

2) I note, as did Dr. Kiper, that none of the new files are viewable on the CF Card report, so they can't be visually examined and compared to their namesake files on the WD HDD, which are, in fact, viewable.
3) I note, as did Dr. Kiper, that none of the MD5 hashes for the new files on the CF Card report match the MD5 hashes on for their namesake files on the WD HDD report. When hashes are different, the files representing those hashes are different.
4) I note, as did Dr. Kiper, that the first CF Card report, 4/11/19 by Flatley, contained file sizes, whereas the second CF Card report, 6/11/19 by Booth, failed to include file sizes, thus preventing a file size comparison.
5) I note, as did Dr. Kiper, that aside from the manipulated files (IMG_0093,4,6,&7 JPGs) discussed in number one above, FTK Toolkit was unable to carve any viewable photo for any of the new files that appear in the 6/11/19 CF Card Report created by Booth. In that same report (6/11/19), FTK was able to carve several dozen viewable photos from the photos listed on the previous report, as well as from unallocated space.
6) I note, as did Dr. Kiper, that "there is nothing besides easily-modifiable file names and file system dates and times that connect the new files in the 06/11 CF Card Report with their namesake photos on the WD HDD report." Not only do I note, but I emphatically agree.

In summation, having reviewed Dr. Kiper's detailed analysis in Appendix D or his report, I concur that the manner in which the files appear in the 6/11/19 CF Card Report is indicative of some unknown person creating batches or groups of "new files" on the CF Card based on file names instead of actual file content, i.e. photographic data. Dr. Kiper cites an example, *" as detailed in Appendix D, the appearance of 20 files (IMG_0081-100) on the second CF Card report implies that the user had taken several pictures of three different subjects, saved them to the CF Card and eventually backed them up to the WD HDD. However, it also requires the user to return to the CF Card, delete only first two photos (by filename) of the first subject, delete no photos of the second subject, and then delete all BUT the first two photos of the third subject. Even more incredibly, the user would have had to delete them in such a way as to prevent the FBI's forensic tool (FTK) from recovering them (e.g. by writing over the sectors). As mentioned earlier, FTK had no problem recovering other deleted files, carving photos from those deleted files, or even recovering viewable photos from the CF Card's unallocated space."* I completely concur with this example and conclusion.

Dr. Kiper concludes this finding with the following, again referring back to Appendix D: *"With the possible exception of IMG_0093-97 files discussed in Finding #1, the new files appearing on the FBI's CF Card forensic report between the 04/11 and 06/11 versions* ***may not even be real digital photos****, since there is no data – no file sizes, no viewable images, no carved photos, no carved thumbnails – to indicate that they are. Nevertheless, these newly added CF card files and metadata match the filenames, dates, and times of files on the WD HDD, indicating that the likely reason for adding these files was to make it appear as though the corresponding files on the WD HDD at one time had originated on the CF card with the dates indicated, consistent with the government's narrative. This is especially significant because other than easily-modifiable EXIF data, there is no forensic evidence linking the hard drive's alleged contraband to the CF*

card. Again, for a detailed analysis of the new files appearing on the 06/11/2019 CF Card report, please see Appendix D." I completely concur.

Finding 3. An unknown person accessed the CF card on 9/19/18, thereby altering file system dates, while it was in the custody of FBI Special Agent Michael Lever.

I observed that there are 16 active files (IMG_0224, 0225, 0227-31, 0233-39, 0241, and 0243 all with JPG extensions) on the CF Card with last accessed dates of 09/19/2018. This is observed on the report GX 521A_Replacement.pdf, generated by FBI CART Examiner Booth. According to the FBI Chain of Custody report, the search warrant was conducted on 03/27/2018 and the Canon camera with the CF Card was seized at that time.

According to the same chain of custody report, SA Michael Lever, lead investigator for the case, signed out the camera and case (the CF Card was found in the latter) on 9/19/2018 and returned same to evidence storage on 9/26/18 a week later. Lever is not a trained digital evidence technician or a CART examiner and is not trained to preview / process / examination original digital evidence, yet he did so. The reason cited when signing out the evidence was "Evidence Review". It was on the first day in Lever's possession, 9/19/2018, that the last accessed dates were registered on the CF Card. Standard procedure is to attach a write blocker between the digital evidence device and the host computer to preserve the integrity of the evidence by preventing any changes whatsoever to the evidence. Clearly someone violated this critical procedure and did not use a write blocker while the CF Card was in Lever's custody. Lever's review of original evidence without training to do so violates the FBI's policies and procedures as set forth in section 3.2.1 in their Digital Evidence Policy guide, as would attaching the CF Card to a computer without a write blocker in place (FBI CART SOP 4.3). FBI policies and procedures are in place to protect the integrity of evidence. It is clear that the CF Card was altered in some fashion while in the custody of SA Lever, the lead investigator in this case, and in clear violation of the FBI's policies and procedures.

As an aside, in any case I ever processed where the evidence was seized by someone other than myself or ever in the possession of another party before I imaged the media, I always sorted by the various timestamps to ensure that no date / time event occurred after it was seized, such as we have in the present case. Often times, particularly in the early days of digital forensics when many officers lacked training in handling digital evidence, law enforcement agencies would seize a computer and 'look at it back at the station' before it was determined to send it to forensics. If I discovered such, I always noted it in my reports and contacted the agency requesting the examination to inquire as to what happened and report back to me. It's something as an examiner you can't overlook, that you must document it, and it would seem that it would be hard to miss in this case. Yet I have seen no such record of any of the FBI examiners documenting this easily detectible spoliation of the data.

Finding 4. Dates of photos on the hard drive were altered through manual intervention. The alterations
seem to be an attempt to account for Daylight Saving Time.

I have reviewed the data in the tables included in Appendix B of Dr. Kiper's report. I have verified the accuracy of that data, including the discrepancies between the last modified times between the EXIF and File System metadata. The fact is, the EXIF last modified time stamp is embedded and does not change simply by moving the file between storage devices, i.e. when moving from the CF Card to the computer. The file system last modified time stamp doesn't change per se. It will come from the FAT file system as local time and then stored on the host computer system, if Windows NTFS file system, in GMT and then displayed according to the local time zone offset and time offset for DST. Regardless, they'll all be treated this way and uniformly. To see discrepancies in the offsets in the tables in Appendix B indicates manipulation / human intervention.

Dr. Kiper states the following:

- *"According to the file listing information in Appendix B, Table 1, there is an inconsistent relationship between two different dates presumably generated by the camera upon creation of the photographs. The EXIF date, generated by the camera, is embedded into the JPG file itself and does not change when the file is copied to another file system. However, the last modified timestamp is saved to the CF card file system, and it may be interpreted differently by another computer, depending on that computer's time zone settings (The Created date is overwritten completely upon copy). I do not have access to the unknown computer into which the photographs were copied, so I have no information about its time zone settings. However, it appears a deliberate effort was made to alter last modified timestamps on the files so they might comport with the Daylight Saving Time, which ended 10/30/2005."*
- *"From IMG_0043 to IMG_0126 the last modified timestamps were one hour behind those of the EXIF dates. On 10/30/2005 starting with IMG_0127 the last modified timestamps of photos were adjusted to be two hours behind, and then on the same day starting with IMG_0138 they were adjusted to be exactly the same as the EXIF dates. Notably, the photos IMG_0127-137 belong to a single folder (Mnp102005\2005-10-29-2350-08) and were the only photos on the WD HDD with this two-hour difference between the Modified dates and the EXIF dates. Nothing outside of human intervention could account for these changes."*
- *"In my experience, there is likewise no legitimate reason a normal user would be making these changes."*

I completely concur with the above, with the added comment that once someone starts down the road of data manipulation, the task undertaken is daunting. It has to be near perfect to avoid detection and the changes must comport to how a computer would create and store data. Little things stand out to an experienced examiner and once the aura of manipulation appears, hard scrutiny follows and more anomalies are discovered, as has happened here.

Finding 5. The metadata of a modified photo, whose numbered filename appears between the alleged
contraband ranges, was manually altered to create the appearance that it had not been modified.

The file, IMG_0175.JPG was found on the CF Card and on the WD HDD. The last modified timestamp for this file in the reports GX 521A_Replacement.pdf (CF Card) and GX 505A.pdf (WD HDD) is 11/10/2005 8:25:04 PM. Since this file is supposedly present on the WD HDD as a backup of the file from the CF Card, the last modified timestamp typically transfers with the file and since they are the same, it would be expected that the file did not change while moving from the CF Card to an unknown computer, and then onto the WD HDD as a backup. An examination of the EXIF data on the file, as it is found on the WD HDD, shows that the Creator of the EXIF data is "Adobe Photoshop Elements 3.0".

When a file is created on the CF Card by the camera, there is no Creator field populated. The Creator field "Abobe Photoshop Elements 3.0" is created on a computer on which that program is installed and when it is used to modify the photo file, typically when the file is copied onto the computer, which had to be the case with this file for it to have been backed up to the WD HDD.

For this Creator field to have been modified to contain "Adobe Photoshop Elements 3.0", then the last modified timestamp would have had to have changed to reflect this modification. It does NOT reflect a change. Rather the modification date has remained unchanged from the time it was created on the CF Card until the time it was supposedly backup up on the WD HDD. This is of course impossible and thus it can be concluded to a scientific certainty that the modification date, the EXIF date, or both have been falsified. The below screenshot shows this file and that its last modified timestamp matches its creation time on the CF Card. Similarly, files taken in the same minute and the minute prior all have modification times that match their creation times, meaning they haven't changed. None of the other files shown in this screenshot have any creator field in their EXIF data, only IMG_0175.JPG and they were all created on the camera at the same approximate time, as shown in the second screenshot below.

Name	Deleted?	Created	Accessed	Modified
IMG_0172.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24
IMG_0173.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24
IMG_0174.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24
IMG_0175.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25
IMG_0176.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25
IMG_0177.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25
IMG_0178.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25

SourceFile	FileName	CreateDate	Model	CanonFirmwareVersion	CreatorTool	ExposureProgram	FileSize	DateTimeOriginal	ImageSize	Quality	FocalLength	ShutterSpeed
/Users/sbunting/Desktop/pics/Attachments/IMG_0129.JPG	IMG_0129.JPG	2005:10:30 04:36:05	Canon EOS 20D	Firmware 2.0.2		Program AE	2.9 MiB	2005:10:30 04:36:05	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0130.JPG	IMG_0130.JPG	2005:10:30 04:36:42	Canon EOS 20D	Firmware 2.0.2		Program AE	2.6 MiB	2005:10:30 04:36:42	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0131.JPG	IMG_0131.JPG	2005:10:30 04:36:55	Canon EOS 20D	Firmware 2.0.2		Program AE	2.7 MiB	2005:10:30 04:36:55	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0132.JPG	IMG_0132.JPG	2005:10:30 04:37:12	Canon EOS 20D	Firmware 2.0.2		Program AE	3.1 MiB	2005:10:30 04:37:12	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0133.JPG	IMG_0133.JPG	2005:10:30 04:37:45	Canon EOS 20D	Firmware 2.0.2		Program AE	2.6 MiB	2005:10:30 04:37:45	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0134.JPG	IMG_0134.JPG	2005:10:30 04:37:58	Canon EOS 20D	Firmware 2.0.2		Program AE	2.9 MiB	2005:10:30 04:37:58	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0135.JPG	IMG_0135.JPG	2005:10:30 04:38:00	Canon EOS 20D	Firmware 2.0.2		Program AE	2.8 MiB	2005:10:30 04:38:00	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0136.JPG	IMG_0136.JPG	2005:10:30 05:39:00	Canon EOS 20D	Firmware 2.0.2		Program AE	2.4 MiB	2005:10:30 05:39:00	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0137.JPG	IMG_0137.JPG	2005:10:30 05:39:06	Canon EOS 20D	Firmware 2.0.2		Program AE	2.1 MiB	2005:10:30 05:39:06	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0138.JPG	IMG_0138.JPG	2005:10:30 16:55:41	Canon EOS 20D	Firmware 2.0.2		Program AE	2.5 MiB	2005:10:30 16:55:41	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0139.JPG	IMG_0139.JPG	2005:10:30 16:55:51	Canon EOS 20D	Firmware 2.0.2		Program AE	2.9 MiB	2005:10:30 16:55:51	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0140.JPG	IMG_0140.JPG	2005:10:30 16:56:21	Canon EOS 20D	Firmware 2.0.2		Program AE	2.8 MiB	2005:10:30 16:56:21	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0141.JPG	IMG_0141.JPG	2005:10:30 16:56:46	Canon EOS 20D	Firmware 2.0.2		Program AE	2.1 MiB	2005:10:30 16:56:46	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0142.JPG	IMG_0142.JPG	2005:10:30 16:57:12	Canon EOS 20D	Firmware 2.0.2		Program AE	2038 KiB	2005:10:30 16:57:12	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0143.JPG	IMG_0143.JPG	2005:10:30 18:01:08	Canon EOS 20D	Firmware 2.0.2		Program AE	3.0 MiB	2005:10:30 18:01:08	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0145.JPG	IMG_0145.JPG	2005:10:30 18:01:19	Canon EOS 20D	Firmware 2.0.2		Program AE	1962 KiB	2005:10:30 18:01:19	3504x2336	Fine	26.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0146.JPG	IMG_0146.JPG	2005:10:30 18:01:28	Canon EOS 20D	Firmware 2.0.2		Program AE	2044 KiB	2005:10:30 18:01:28	3504x2336	Fine	38.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0147.JPG	IMG_0147.JPG	2005:10:30 18:02:08	Canon EOS 20D	Firmware 2.0.2		Program AE	2.3 MiB	2005:10:30 18:02:08	3504x2336	Fine	38.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0148.JPG	IMG_0148.JPG	2005:10:30 18:02:15	Canon EOS 20D	Firmware 2.0.2		Program AE	2.1 MiB	2005:10:30 18:02:15	3504x2336	Fine	38.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0149.JPG	IMG_0149.JPG	2005:10:30 18:02:22	Canon EOS 20D	Firmware 2.0.2		Program AE	2.1 MiB	2005:10:30 18:02:22	3504x2336	Fine	38.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0164.JPG	IMG_0164.JPG	2005:11:10 20:22:18	Canon EOS 20D	Firmware 2.0.2		Program AE	2.7 MiB	2005:11:10 20:22:18	3504x2336	Fine	17.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0165.JPG	IMG_0165.JPG	2005:11:10 20:22:30	Canon EOS 20D	Firmware 2.0.2		Program AE	2.4 MiB	2005:11:10 20:22:30	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0168.JPG	IMG_0168.JPG	2005:11:10 20:23:12	Canon EOS 20D	Firmware 2.0.2		Program AE	2.3 MiB	2005:11:10 20:23:12	3504x2336	Fine	35.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0169.JPG	IMG_0169.JPG	2005:11:10 20:23:26	Canon EOS 20D	Firmware 2.0.2		Program AE	2.2 MiB	2005:11:10 20:23:26	3504x2336	Fine	17.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0172.JPG	IMG_0172.JPG	2005:11:10 20:24:19	Canon EOS 20D	Firmware 2.0.2		Program AE	2.0 MiB	2005:11:10 20:24:19	3504x2336	Fine	17.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0174.JPG	IMG_0174.JPG	2005:11:10 20:24:47	Canon EOS 20D	Firmware 2.0.2		Program AE	2.1 MiB	2005:11:10 20:24:47	3504x2336	Fine	17.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0175.JPG	IMG_0175.JPG	2005:11:10 20:25:04	Canon EOS 20D	Firmware 2.0.2	Adobe Photoshop Elements 3.0	Program AE	2.4 MiB	2005:11:10 20:25:04	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0176.JPG	IMG_0176.JPG	2005:11:10 20:25:11	Canon EOS 20D	Firmware 2.0.2		Program AE	1964 KiB	2005:11:10 20:25:11	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0177.JPG	IMG_0177.JPG	2005:11:10 20:25:35	Canon EOS 20D	Firmware 2.0.2		Program AE	2.5 MiB	2005:11:10 20:25:35	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0178.JPG	IMG_0178.JPG	2005:11:10 20:25:54	Canon EOS 20D	Firmware 2.0.2		Program AE	2.2 MiB	2005:11:10 20:25:54	3504x2336	Fine	22.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0179.JPG	IMG_0179.JPG	2005:11:10 20:26:04	Canon EOS 20D	Firmware 2.0.2		Program AE	2.2 MiB	2005:11:10 20:26:04	3504x2336	Fine	56.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0180.JPG	IMG_0180.JPG	2005:11:10 20:26:22	Canon EOS 20D	Firmware 2.0.2		Program AE	2.4 MiB	2005:11:10 20:26:22	3504x2336	Fine	56.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0181.JPG	IMG_0181.JPG	2005:11:10 20:26:25	Canon EOS 20D	Firmware 2.0.2		Program AE	2.8 MiB	2005:11:10 20:26:25	3504x2336	Fine	56.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0182.JPG	IMG_0182.JPG	2005:11:10 20:26:29	Canon EOS 20D	Firmware 2.0.2		Program AE	3.0 MiB	2005:11:10 20:26:29	3504x2336	Fine	56.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0183.JPG	IMG_0183.JPG	2005:11:10 20:27:33	Canon EOS 20D	Firmware 2.0.2		Program AE	2.4 MiB	2005:11:10 20:27:33	3504x2336	Fine	17.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0194.JPG	IMG_0194.JPG	2005:12:19 00:37:58	Canon EOS 20D	Firmware 2.0.2		Program AE	2.4 MiB	2005:12:19 00:37:58	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0197.JPG	IMG_0197.JPG	2005:12:19 00:38:20	Canon EOS 20D	Firmware 2.0.2		Program AE	2.5 MiB	2005:12:19 00:38:20	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0198.JPG	IMG_0198.JPG	2005:12:19 00:38:28	Canon EOS 20D	Firmware 2.0.2		Program AE	2.7 MiB	2005:12:19 00:38:28	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0199.JPG	IMG_0199.JPG	2005:12:19 00:38:55	Canon EOS 20D	Firmware 2.0.2		Program AE	2.6 MiB	2005:12:19 00:38:55	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0203.JPG	IMG_0203.JPG	2005:12:26 02:59:44	Canon EOS 20D	Firmware 2.0.2		Program AE	2.4 MiB	2005:12:26 02:59:44	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0204.JPG	IMG_0204.JPG	2005:12:26 02:59:50	Canon EOS 20D	Firmware 2.0.2		Program AE	2.3 MiB	2005:12:26 02:59:50	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0205.JPG	IMG_0205.JPG	2005:12:26 03:00:42	Canon EOS 20D	Firmware 2.0.2		Program AE	2.5 MiB	2005:12:26 03:00:42	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0206.JPG	IMG_0206.JPG	2005:12:26 03:00:49	Canon EOS 20D	Firmware 2.0.2		Program AE	3.1 MiB	2005:12:26 03:00:49	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0207.JPG	IMG_0207.JPG	2005:12:26 03:01:40	Canon EOS 20D	Firmware 2.0.2		Program AE	2.0 MiB	2005:12:26 03:01:40	3504x2336	Fine	17.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0208.JPG	IMG_0208.JPG	2005:12:26 03:01:46	Canon EOS 20D	Firmware 2.0.2		Program AE	2.2 MiB	2005:12:26 03:01:46	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0209.JPG	IMG_0209.JPG	2005:12:30 17:56:05	Canon EOS 20D	Firmware 2.0.2		Program AE	2.1 MiB	2005:12:30 17:56:05	3504x2336	Fine	85.0 mm	1/60
/Users/sbunting/Desktop/pics/Attachments/IMG_0210.JPG	IMG_0210.JPG	2005:12:30 17:56:11	Canon EOS 20D	Firmware 2.0.2		Program AE	2.4 MiB	2005:12:30 17:56:11	3504x2336	Fine	85.0 mm	1/60

As Dr. Kiper points out, all the photos contained on the CF Card that are created by the Canon camera have a fixed length for their EXIF data, which ends where the thumbnail offset begins. The thumbnails for all these Canon-camera created photos start at the very next byte, which is byte offset 9728, hence all thumbnail files carved from these files are named Carved [9728].jpeg. There is, however, one exception, which is file IMG_0175.JPG, which contains the Creator field “Adobe Photoshop Elements 3.0”. Its carved thumbnail is named “Carved [9104].jpg”. Its thumbnail starts at a different byte offset because its EXIF data is different from all the others when it should NOT be so.

There is no explanation as to how the camera could create this anomaly. It could not. If the computer were used to edit the photo with Adobe Photoshop Elements directly while it was on the CF card, the Creator field could have been so created, however it would have modified the photo and the modification date, which did not occur. Therefore the only reasonable explanation is manipulation of the data, given all the other anomalies and that they CF card was accessed and data altered while in FBI possession, which is an established fact. Thus the likely explanation is, as Dr. Kiper suggests, residual data that was overlooked during the cleanup phase of the digital evidence manipulation process.

Finding 6. The folders containing the alleged contraband and others that supported the dating of the
photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.

For finding #6, Dr. Kiper states the following:
"At trial the government acknowledged that the upper level folders, such as Df101905, were created by a human when FE Booth testified, "Yes, it looks like someone put the date and time associated with two letters" (p. 4984).

However, during court proceedings the government repeatedly asked FE Booth to confirm both the upper level and lower level folder names (such as 2005-11-02-0422-20) "roughly" correspond to the original date and time contained in the EXIF data of files in those folders (e.g., pp. 4852-56). The clear implication was that these folder names could be relied upon to corroborate the values in the EXIF data. In fact, during closing arguments the government stated, "Brian Booth testified that the most reliable metadata that the FBI could obtain from the images on the Western digital hard drive, said that they were taken exactly when the folders stated they were taken" (p. 5371).

The folders could not have been generated by the Canon camera, since that camera creates folders named "CANON100" to store the first 100 photos, "CANON200" for the second 100 photos, and so on. This folder naming convention appears in the file paths of both of the government's FTK reports of the CF card, dated 04/11/2019 and 06/11/2019.

Testing has demonstrated that Adobe Photoshop Elements can indeed create folder names with the YYYY-MM-DD-HHMM-SS nomenclature, but the date and time is based upon the current system clock at the time the photos were imported into Adobe Photoshop, not on the created timestamps of the photos themselves. This fact reveals how the folder names were subsequently manipulated.

According to the date/time nomenclature, for example, the folders "2005-10-19-0727-57" and "2005-10-19-0727-59" would have had to have been created two seconds apart (7:27:57 AM and 7:27:59 AM, respectively). These folders reside under separate and uniquely named parent folders, "Df101905" and "Msk101905," respectively (See Appendix A, Figure 5). The latter portion of these folder names could not possibly correspond to realistic folder creation times because two seconds is not enough time to manually select nine files, IMG_0090-98, copy them into the Df101905 folder, and then manually select another eleven files, IMG_0079-89, and manually navigate to the Msk101905 folder and save them there.

In addition, I discovered a Thumbs.db file in each of the folders "2005-10-19-0727-57" and "2005-10-19-0727-59." In earlier versions of Windows, a Thumbs.db was automatically generated in a folder to contain previews of each file in the folder. However, I discovered that the Thumbs.db file in each of the "2005-10-19-0727-57" and "2005-10-19-0727-59" folders contain previews of the full range of photos IMG_0079-98. This means that all of those photos used to reside in a single folder in the past, and some time later they were divided and placed into their current locations, which are: IMG_0090-98 into the / Df101905/2005-10-19-0727-57/ folder and IMG_0079-89 into the /Msk101905/2005-10-19-0727-59/ folder. The fact that all photo previews were contained in both Thumbs.db files likely indicates that an earlier folder, containing all IMG_0079-98 photos, was duplicated, the resulting folders were

renamed and placed into the Df101905 and Msk101905 folders, and then unwanted photos from each folder were removed. No special skills are required to move files and rename folders in the way I just described, and people often do so to organize photos according to subject matter.

It is certain that some of the timestamped folder names were manually manipulated, such as the ones described above. Given the ease with which one can alter folder names, it is possible the names of the folders containing alleged contraband (2005-11-02-0422-20 and 2005-11-24-0814-46) were manually set in a way that aligns with the prosecution's narrative that the photos were taken in November 2005, and therefore the subject would have been fifteen years old, according to the trial record. At the very least, the dates and times indicated in these folder names cannot be relied upon to determine or corroborate the creation dates of the photos contained in them."

I have confirmed the testimony by Booth referenced in the first two bullets, including the closing arguments quoting his testimony citing the reliability of the metadata of the folder names themselves in establishing when the photos were taken. The Canon camera does not create the folder structure referred to in this finding, rather, as Dr. Kiper states, the Camera creates a folder naming convention such as CANON100, CANON200, etc or 100CANON, 200CANON, etc. These folders contain batches of files based on quantity, not date / time. Thus the camera did not create this folder structure. I can confirm that Adobe Photoshop Elements can create a folder structure such as the one discussed, i.e. YYYY-MM-DD-HHMM-SS, but said date / time would reflect not EXIF dates / times, but rather the system date / time of the import. Other tools are available to create this folder pattern based on EXIF data (AMOK EXIF Sorter, NameEXIF, etc).

In bullet six, Dr. Kiper discusses the import of a thumbs.db file that establishes that the file series IMG_0079-98 were at one time all in the same folder. I located the thumbs.db file to which he refers. The thumbnail pictures are of two distinctly different women and that they are in the same thumbs.db establishes there were all, pictures of both women, at one time in the same folder. They have been since segregated into two separate folders, 2005-10-19-0727-57 and 2005-10-19-0727-59, the former for the brunette and the latter for the woman with auburn hair.

Based on my above observations and analysis, I fully concur with Dr. Kiper's analysis, reasoning, and conclusions in this finding. I emphatically agree that these dates and times indicated by these folder names, at the very least, cannot be relied upon to establish or corroborate the creation dates of the photos contained in them. These folders were either created from unreliable metadata or from manual creation / manipulation, neither of which can be considered reliable for establishing creation dates / times for the photos contained therein.

Finding 7. The photos in this case, including the alleged contraband photos, appear to be on the hard

drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates.

Dr. Kiper states:

"According to the file listing of a forensically imaged Western Digital hard drive (WD HDD), on 03/30/2009 a backup was made of a Dell Inspiron 700M and given the folder name "BKP.DellInspiron700M-20090330." Also on 03/30/2009 a PowerMac was backed up to the folder "BKP.PowerMac8.2-2009-0330." Unsurprisingly, all the Created dates in these folders were 03/30/2009 (or very early 03/31/2009), the backup date identified in the folder name (see Appendix A, Figure 4). By contrast, all the files in the unknown computer ("Dell Dimension") backup folder ("BKP.DellDimension8300-20090330") have a Created date of 07/26/2003, and the backup folder has a last Accessed date of 07/28/2003, despite the folder name indicating the same backup date as the others (03/30/2009).

When files are copied from one file system to another, their Created dates are changed to the current clock time of the machine hosting the receiving file system. If all clocks are accurate, then the created times of these copied files will necessarily be AFTER the last modified times.

In this case, however, all the files in the unknown computer backup ("BKP.DellDimension8300-20090330") have a Created date of 07/26/2003, while most of their Modified dates are from October 2005 and later. This observation indicates the system clock was rolled back to 2003 before copying these files manually onto the hard drive.

Sometimes the computer's CMOS battery – which enables the computer to retain information after shutdown such as system time – goes bad, resulting in the system clock being reset to a default date, such as 01/01/2003 [NOTE]. However, the computer will continue to reset the system clock to that date every time the computer powers up. Therefore, a bad CMOS battery cannot explain the system clock set to 07/26/2003 for the creation date of the files in the folder whose name, as mentioned previously, indicates a 03/30/2009 backup. It also fails to explain the creation dates of several hundred (mostly music) files copied to the WD HDD between 08/08/2003 and 08/18/2003 that were NOT located in the "BACKUPS" folder.

The rolling back of the system clock is more likely the result of someone who was trying to backdate the folder content and make this folder appear to be a legitimate backup folder but may not have considered how and when file system dates are normally updated.
There are other significant anomalies in this backup folder that showcase the failed effort to create the appearance of an automated backup:

The Dell Inspiron backup contains more than 15,000 files, while Dell Dimension backup was backed up in two separate copy operations, in total less than 500 files.

The Dell Inspiron backup included several directories, such as Desktop, Favorites, and My Documents, while the Dell Dimension backup initially only included the Studies folder, containing the images in question. It is uncommon for a user to choose to primarily back up a particular folder (in this case, the "Studies" folder) from an entire desktop system, while ignoring more common file storage locations such as My Documents. To accept the legitimacy of this backup one would need to believe a highly improbable scenario where the user made a concerted effort to back up a folder containing his contraband, and specifically this folder, from an entire desktop system. In a likely attempt to create the appearance of a legitimate backup – more than an hour after the "Studies" files were copied – a Symantec folder with one file, and about 150 songs were added to the backup folder.

NOTE: Although the "factory default" date could theoretically be any date, I have never seen one that is NOT on the first day of the month, either in January or December of the year of manufacture."

I have reviewed the date / time discrepancies set forth in bullet one of this finding. I confirm the date and time discrepancies delineated by Dr. Kiper. It is important to emphasize that, in particular, when creating a backup, the creation date of that backup will be later than the last modified timestamps of any of the files contained within that backup, assuming all time clocks creating those timestamps are accurate.

The folder names for the backups purport to indicate when the backups were made, yet for the backup containing the contraband files, the actual creation date of the backup is over two years sooner than the last modified timestamps of the contraband files, whereas the created timestamp of the backup should be after the latest last modification time in the backup. At the very least, the timestamps are totally unreliable.

I concur completely with Dr. Kiper's finding, i.e. his analysis of the data, his observations, his logic, and his conclusion that the most plausible explanation is that the folder containing the alleged contraband was planted on the hard drive, to look like a legitimate automated computer backup had copied the alleged contraband onto the hard drive.

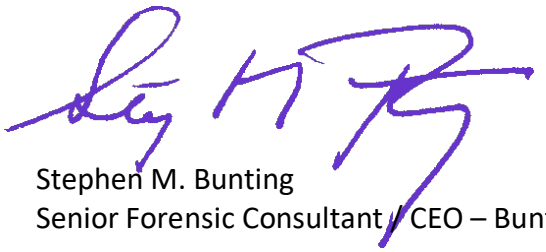
Conclusion

Dr. Kiper concludes with the following: "*the forensic evidence shows that folder names and dates (key facts upon which the prosecution's argument relied) were manually altered, and the entire backup folder to which the alleged contraband belonged was manipulated. While it is impossible to determine exactly when the information on the WD HDD was altered, it is a scientific certainty that data on the CF card were added and/or modified while the device was in FBI custody*."

I could not agree more with Dr. Kiper's final conclusion. The prosecution relied upon the folder names and dates as a basis for establishing when photos were created and those dates / times were manipulated. The evidence is tainted and unreliable. They also relied upon EXIF dates / times, falsely claiming EXIF metadata to be reliable when, in fact, it is easy to modify. I agree

that the information on the WD HDD has been altered, but we currently lack the data and/or access to assess when such occurred. Finally, and probably most critically, it is a scientific certainty that data on the CF Card were added and/or modified while the CF Card was in FBI custody, specifically while signed out to SA Michael Lever, the lead investigator for this case.

Respectfully Submitted,



Stephen M. Bunting
Senior Forensic Consultant / CEO – Bunting Digital Forensics, LLC

Appendix A - Affidavit_with_Reports_04-25-2022.pdf
Appendix B - Flatley_vs_Booth_Analysis_with_Affidavit_sm.pdf
Appendix C – Stephen Bunting Curriculum Vitae (Bunting BDF CV updated 2022 Sept 11.pdf)

Appendix A

Affidavit of Dr. James Richard Kiper, Ph.D.

State of Florida
County of Leon

COMES NOW Dr. James Richard Kiper, Ph.D., being first duly sworn, under oath, and states that the contents of the following attached reports, including their appendices, and exhibits are true and correct statements of relevant facts and his opinions in the case of United States v. Keith Raniere et. al., in the United States District Court, Eastern District of New York, Case #: 1:180-cr-00204-NGG-VMS, to the best of his knowledge and belief:

- Summary of Technical Findings
- Summary of Process Findings
- Analysis of the Testimony of Special Agent Christopher Mills
- Expert Opinion Regarding Time to Review Digital Evidence

Signature: _____

Address: 818 Shannon Street
Tallahassee, Florida 32305

SUBSCRIBED AND SWORN TO before me this 25 day of April, 2022, by James Kiper.

_____
NOTARY PUBLIC FOR FLORIDA

Michael Jordan
Comm. # GG366579
Expires: October 1, 2023
Bonded Thru Aaron Notary

My Commission Expires: 10/1/23

J. Richard Kiper, PhD, PMP

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

Summary of Technical Findings

Professional Background

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have an in-depth knowledge of FBI digital evidence examination procedures and policies.

Review of Evidence

On May 21, 2021, I signed the Protective Order Regarding Discovery in U.S. v. Raniere, et al., 18 CR 204 (NGG) and was subsequently provided access to certain evidence in this case. My review of evidence includes court testimony, a hard drive copy of logical files, and examination reports generated by members of the FBI's Computer Analysis Response Team (CART). Based on my review, I discovered specific actions that were taken to manually alter the evidence, in support of the government's narrative that photos were taken by a Canon EOS 20D camera (GX 520), saved to a Lexar CF card (GX 524), copied to an unknown computer, and then backed up to a Western Digital hard disk drive (GX 503). In this report I will refer to the latter two items as the CF Card and the WD HDD.

In my 20 years serving as an FBI agent, I have never observed or claimed that an FBI employee tampered with evidence, digital or otherwise. But in this case, I strongly believe the multiple, intentional alterations to the digital information I have discovered constitute evidence manipulation. And when so many human-generated alterations happen to align with the government's narrative, I believe any reasonable person would conclude that evidence tampering had taken place. My analysis demonstrates that some of these alterations definitely took place while the devices were in the custody of the FBI. Therefore, in the absence of any other plausible explanation it is my expert opinion that the FBI must have been involved in this evidence tampering.

Key Findings

1. Some digital photo files found on the CF card had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people. Moreover, these same CF card files contained thumbnail pictures from another existing set of photos, thus proving manual alteration of the CF Card contents.
2. Additional files appeared on the FBI's forensic report of the CF Card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the CF Card and the WD HDD.
3. An unknown person accessed the CF card on 9/19/18, thereby altering file system dates, while it was in the custody of FBI Special Agent Michael Lever.
4. Dates of photos on the hard drive were altered through manual intervention. The alterations seem to be an attempt to account for Daylight Saving Time.
5. The metadata of a modified photo, whose numbered filename appears between the alleged contraband ranges, was manually altered to create the appearance that it had not been modified.
6. The folders containing the alleged contraband and others that supported the dating of the photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.
7. The photos in this case, including the alleged contraband photos, appear to be on the hard drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates.

Finding 1: Some digital photo files found on the CF card had the same filenames and date/time stamps as their supposed backups on the WD HDD, yet they depicted two different people. Moreover, these same CF card files contained thumbnail pictures from another existing set of photos, thus proving manual alteration of the CF Card contents.

- As further explained in Finding #2, photos named IMG_0093.JPG, IMG_0094.JPG, IMG_0096.JPG and IMG_0097.JPG (hereinafter IMG_0093-97) were among those that appeared on the FBI's WD HDD forensic report, but they did not initially appear on the CF Card forensic report generated on 04/11/2019. Subsequently, however, on 06/11/2019 the FBI created another version of the CF Card forensic report wherein these and other photo files were included. It is important to note that neither the IMG_0093-97 files, nor any other of the newly-added files, were **viewable** as photo images in the 06/11/2019 forensic report of the CF Card.
- The government's narrative requires that the IMG_0093-97 files on the second CF Card report be identical to the IMG_0093-97 files found in the WD HDD report, because photos created

on the CF Card were supposedly backed up to the WD HDD unaltered. Indeed, they have identical file names, identical Modified dates, and (presumably) identical EXIF data, including the date taken, camera model, and serial number[1]. However, they cannot be identical photo files because their MD5 hashes ("digital fingerprints") do not match (See **Appendix A**, Figure 3).

- Moreover, a content review of the files reveals the subjects of the photographs found on the two devices are actually two different people. Although the IMG_0093-97 files were not viewable as photos in the 06/11/2019 CF Card report, their forensically recovered carved thumbnail photos were viewable, and they depicted a **blonde** woman. By contrast, the IMG_0093-97 files on the WD HDD report were viewable photographs and they depicted a **brunette** woman. Again, the two sets of IMG_0093-97 files share the same file names and the same last Modified dates and times – to the second. *This would mean the same camera, with the same serial number, took two different photographs of two different subjects at precisely the same time and assigned them the same file name.* This is impossible, of course, so the presence of these files indicates the manipulation of the content and metadata for these photos.
- In fact, a detailed analysis of the carved file listings for each device revealed that IMG_0093, IMG_0094, IMG_0096, and IMG_0097 found on the CF Card are not only different from their namesakes on the WD HDD, but they also **contain the same thumbnail images** as those of IMG_0180, IMG_0181, IMG_0182, and IMG_183, *respectively*. This surprising observation points to someone creating copies of IMG_0180–183 and then making changes to them on the CF card, including changing their file names to IMG_0093, IMG_0094, IMG_0096, and IMG_0097. These intentional alterations likely resulted in the files being unviewable on the 06/11/2019 forensic report, but it did not destroy the thumbnail images left over from the IMG_0180–0183 photos. It is likely the custodians of the CF Card who added these files, the case agents or their associates, repurposed the IMG_0180–183 files because at that time they did not have physical control of the WD HDD or its files. The FBI's Case Agent Investigative Review (CAIR) system enabled the case agents to review the WD HDD evidence and bookmark items, but it prevented them from exporting any information from the evidence. Please refer to **Appendix C** for an in-depth analysis of the carved files found in the WD HDD and CF Card forensic (FTK) reports.
- The intentional modification of the IMG_0093-97 files on the CF Card report cannot be explained by normal use of the camera or CF Card. In the context of this case, the alterations are best explained by the intentions of an unknown actor attempting to create a stronger relationship between the CF Card photo files and the WD HDD that supposedly contained their backups. These actions will be further explained in Finding 2.

[1] As noted in my Process Findings, neither the two forensic images of the CF card, nor the EXIF data from files in the associated FTK reports, were produced during discovery. However, I was able to determine that photographic data from IMG_0180 to IMG_0183, were actually found in the newly-added photos on the CF report with file names IMG_0093, IMG_0094, IMG_0096, and IMG_0097 (See **Appendix C**). If I had full access to the CF card data, it is reasonable to assume I would find the same EXIF data in those files as well.

Finding 2: Additional files appeared on the FBI's forensic report of the CF Card, between 4/11/19 and 6/11/19, in an apparent attempt to create a stronger relationship between the CF Card and the WD HDD.

- On 4/11/19, FBI forensic examiner Stephen Flatley created a forensic copy of the CF card, processed the data, and generated a forensic report using AccessData Forensic Toolkit (FTK), also known as AD LAB. The report listed active files present on the CF card, as well as those that had been deleted.
- On 6/11/19, five weeks into the trial and one day before he took the stand, FBI Examiner Brian Booth created *another* forensic copy and *another* FTK report of the same CF card. In the FBI, this is considered a reexamination and is prohibited by policy (see my Process Findings report). However, in this second report there were **new files** present in the file listing that **were not on the previous report**: Namely, IMG_0042, IMG_0081–IMG_0100, IMG_0172–IMG_0179, and IMG_0193–IMG_200.
- In the FBI, CART examiners generate FTK reports, which contain file listings, graphics, and exported files that were identified and bookmarked by the case agent or CART examiner. At times, new reports are generated from *existing forensic copies* of the same device, when the facts of the investigation change or when a new forensic tool becomes available. In this case, however, the difference between the two FTK reports cannot be attributed to the use of a different tool, because both examiners used the same tool and version number: AccessData Forensic Toolkit, Version 6.3.1.26.
- The appearance of new files on a subsequent forensic report does not, by itself, necessarily mean that files were added to the original device. However, I have generated hundreds of FTK reports for the FBI, and I can think of no legitimate reason for new files to appear on a subsequent FTK report generated by the same software and version number, working under the same set of facts, on the same piece of evidence, which is supposed to be preserved and immutable from the time of collection.
- In fact, there are several reasons to suspect that the new files appearing on the 06/11/2019 CF Card report did not legitimately originate on the CF Card itself:
    - None of the new files are viewable in the 06/11/2019 report, while all the files previously appearing on the 04/11/2019 report are viewable.
    - None of the new files are viewable on the CF Card report, so they cannot be visually compared with their namesakes on the WD HDD, which **are** viewable.
    - None of the **MD5 hashes** for the new files on the CF Card report match their namesakes on the WD HDD report. Mismatched MD5 hashes means they are not the same files.
    - Unlike the first 04/11 CF card report, the second 06/11 CF Card report **omitted the file sizes** for the photos, thereby preventing even a file size comparison of the new files with their namesakes on the WD HDD.
    - Aside from the manipulated IMG_0093-97 files discussed in Finding #1, the FBI's

forensic tool (FTK) was **unable to carve a single viewable photo** from any of the new files appearing on the 06/11 CF Card report. In that same report, by contrast, FTK was able to carve out several dozen viewable photos from the CF Card's previous photos as well as from unallocated space (with no links to specific files).

- To summarize, there is nothing besides easily-modifiable file names and file system dates and times that connect the new files in the 06/11 CF Card report with their namesake photos on the WD HDD report.

- Moreover, the way the new files appear on the 06/11/2019 CF Card report is indicative of someone creating large swaths of "new files" on the CF Card based on file names, rather than on content. For example, as detailed in **Appendix D**, the appearance of 20 files (IMG_0081-100) on the second CF Card report implies that the user had taken several pictures of three different subjects, saved them to the CF Card and eventually backed them up to the WD HDD. However, it also requires the user to return to the CF Card, delete only first two photos (by filename) of the first subject, delete no photos of the second subject, and then delete all BUT the first two photos of the third subject. Even more incredibly, the user would have had to delete them in such a way as to prevent the FBI's forensic tool (FTK) from recovering them (e.g. by writing over the sectors). As mentioned earlier, FTK had no problem recovering other deleted files, carving photos from those deleted files, or even recovering viewable photos from the CF Card's unallocated space.
- With the possible exception of IMG_0093-97 files discussed in Finding #1, the new files appearing on the FBI's CF Card forensic report between the 04/11 and 06/11 versions **may not even be real digital photos**, since there is no data – no file sizes, no viewable images, no carved photos, no carved thumbnails – to indicate that they are. Nevertheless, these newly added CF card files and metadata match the filenames, dates, and times of files on the WD HDD, indicating that the likely reason for adding these files was to make it appear as though the corresponding files on the WD HDD at one time had originated on the CF card with the dates indicated, consistent with the government's narrative. This is especially significant because other than easily-modifiable EXIF data, there is no forensic evidence linking the hard drive's alleged contraband to the CF card. Again, for a detailed analysis of the new files appearing on the 06/11/2019 CF Card report, please see **Appendix D**.

Finding 3: An unknown person accessed the CF card on 9/19/18, thereby altering file system dates, while it was in the custody of FBI Special Agent Michael Lever.

- According to the CF card file listing (see **Appendix A**, Figure 1), the Accessed dates for *all the active files* were changed to 09/19/2018 (The rest of the files are recoverable deleted files). At a minimum, this finding demonstrates that file system dates on the CF card were altered on at least one occasion, 09/19/2018, six months after it was collected by the FBI on 03/27/2018.
- The presence of updated accessed dates also demonstrates the FBI did not use a write blocker to preserve the evidence, which is a "critical procedure" according to FBI CART SOP 4.3 (see my Process Findings).

- According to the FBI Chain of Custody for the Camera and CF card, Case Agent Michael Lever checked out these items from Evidence Control on 09/19/2018 and returned them on 09/26/2018 (see **Appendix A**, Figure 2). SA Lever recorded his purpose for accepting custody as "Evidence Review." Therefore, SA Lever is most likely the person who accessed the CF card on 09/19/2018 without a write blocker. As I explain in my Process Findings report, this unauthorized access not only changed the evidence but it also violated FBI digital evidence handling policy.

Finding 4: Dates of photos on the hard drive were altered through manual intervention. The alterations seem to be an attempt to account for Daylight Saving Time.

- According to the file listing information in **Appendix B**, Table 1, there is an inconsistent relationship between two different dates presumably generated by the camera upon creation of the photographs. The EXIF date, generated by the camera, is embedded into the JPG file itself and does not change when the file is copied to another file system. However, the Modified date is saved to the CF card file system, and it may be interpreted differently by another computer, depending on that computer's time zone settings (The Created date is overwritten completely upon copy). I do not have access to the unknown computer into which the photographs were copied, so I have no information about its time zone settings. However, it appears a deliberate effort was made to alter Modified dates on the files so they might comport with the Daylight Saving Time, which ended 10/30/2005.
- From IMG_0043 to IMG_0126 the Modified dates were one hour behind those of the EXIF dates. On 10/30/2005 starting with IMG_0127 the Modified dates of photos were adjusted to be **two hours** behind, and then on the same day starting with IMG_0138 they were adjusted to be **exactly the same** as the EXIF dates. Notably, the photos IMG_0127-137 belong to a single folder (Mnp102005\2005-10-29-2350-08) and were the only photos on the WD HDD with this two-hour difference between the Modified dates and the EXIF dates. Nothing outside of human intervention could account for these changes.
- In my experience, there is likewise no legitimate reason a normal user would be making these changes.

Finding 5: The metadata of a modified photo, whose numbered filename appears between the alleged contraband ranges, was manually altered to create the appearance that it had not been modified.

- The Modified date of **IMG_0175** on the hard drive matches the Modified date of IMG_0175 recovered on the CF card, which would normally indicate that IMG_0175 was downloaded from the CF card onto an unknown computer and then copied to the hard drive without ever being modified.
- However, the EXIF CreatorTool value of IMG_0175 is set to "Adobe Photoshop Elements

3.0," which indicates that Adobe Photoshop was used to open and modify the file data. The Adobe Photoshop value could not have been set by the camera, and it was not observed in the EXIF data of any other photo. Since the EXIF data is part of the content portion of the file, its modification must result in an updated Modified date. The fact that the file's Modified dates are exactly the same on both devices - in the face of obvious modification - indicates the dates have been manually altered to be the same (See **Appendix A**, Figure 6).

- Modified dates are normally unaltered when copying to a new file system. Therefore, the act of altering a Modified date when content modification occurred reveals an intent by the user to conceal the file modification by coordinating the Modified dates between the CF card and the hard drive.
- The uniqueness of the EXIF data in the IMG_0175 file is also reflected in the thumbnail photo that was carved from it on the HDD. Every other carved thumbnail in this case is named "Carved [9728].jpeg," meaning it was carved at the end of the fixed length EXIF portion of the file located at byte offset 9728 (See **Appendix C** for a more detailed explanation). However, the thumbnail carved from IMG_0175 is named "Carved [9104].jpeg," meaning the EXIF data in this file is different from all the others.
- The fact that only one file, IMG_0175, still contains the EXIF CreatorTool value set at "Photoshop Adobe Elements 3.0" is likely due to an oversight on the part of the person altering the EXIF data. Like the other files in the WD HDD, it contains the EXIF model and serial number of the camera, but none of the other files contains a reference to Photoshop.

Finding 6: The folders containing the alleged contraband and others that supported the dating of the photos to 2005 appear automatically named after exact dates and times in 2005. However, at least some of these timestamped folder names were manually altered.

- At trial the government acknowledged that the upper level folders, such as Df101905, were created by a human when FE Booth testified, "Yes, it looks like someone put the date and time associated with two letters" (p. 4984).
- However, during court proceedings the government repeatedly asked FE Booth to confirm both the upper level and lower level folder names (such as 2005-11-02-0422-20) "roughly" correspond to the original date and time contained in the EXIF data of files in those folders (e.g., pp. 4852-56). The clear implication was that these folder names could be relied upon to corroborate the values in the EXIF data. In fact, during closing arguments the government stated, "Brian Booth testified that the most reliable metadata that the FBI could obtain from the images on the Western digital hard drive, said that they were taken exactly when the folders stated they were taken" (p. 5371).
- The folders could not have been generated by the Canon camera, since that camera creates folders named "CANON100" to store the first 100 photos, "CANON200" for the second 100 photos, and so on. This folder naming convention appears in the file paths of both of the

government's FTK reports of the CF card, dated 04/11/2019 and 06/11/2019.

- Testing has demonstrated that Adobe Photoshop Elements can indeed create folder names with the YYYY-MM-DD-HHMM-SS nomenclature, but the date and time is based upon the current system clock at the time the photos were imported into Adobe Photoshop, not on the created times of the photos themselves. This fact reveals how the folder names were subsequently manipulated.
- According to the date/time nomenclature, for example, the folders "2005-10-19-0727-57" and "2005-10-19-0727-59" would have had to have been created **two seconds apart** (7:27:57 AM and 7:27:59 AM, respectively). These folders reside under separate and uniquely named parent folders, "Df101905" and "Msk101905," respectively (See **Appendix A**, Figure 5). The latter portion of these folder names could not possibly correspond to realistic folder creation times because two seconds is not enough time to manually select nine files, IMG_0090-98, copy them into the Df101905 folder, and then manually select another eleven files, IMG_0079-89, and manually navigate to the Msk101905 folder and save them there.
- In addition, I discovered a Thumbs.db file in each of the folders "2005-10-19-0727-57" and "2005-10-19-0727-59." In earlier versions of Windows, a Thumbs.db was automatically generated in a folder to contain previews of each file in the folder. However, I discovered that the Thumbs.db file in each of the "2005-10-19-0727-57" and "2005-10-19-0727-59" folders contain previews of **the full range of photos IMG_0079-98**. This means that all of those photos used to reside in a single folder in the *past*, and some time later they were divided and placed into their *current* locations, which are: IMG_0090-98 into the / Df101905/2005-10-19-0727-57/ folder and IMG_0079-89 into the /Msk101905/2005-10-19-0727-59/ folder. The fact that all photo previews were contained in both Thumbs.db files likely indicates that an earlier folder, containing all IMG_0079-98 photos, was duplicated, the resulting folders were renamed and placed into the Df101905 and Msk101905 folders, and then unwanted photos from each folder were removed. No special skills are required to move files and rename folders in the way I just described, and people often do so to organize photos according to subject matter.
- It is certain that some of the timestamped folder names were manually manipulated, such as the ones described above. Given the ease with which one can alter folder names, it is possible the names of the folders containing alleged contraband (2005-11-02-0422-20 and 2005-11-24-0814-46) were manually set in a way that aligns with the prosecution's narrative that the photos were taken in November 2005, and therefore the subject would have been fifteen years old, according to the trial record. At the very least, the dates and times indicated in these folder names cannot be relied upon to determine or corroborate the creation dates of the photos contained in them.

Finding 7: The photos in this case, including the alleged contraband photos, appear to be on the hard drive from an automated computer backup in 2009. But in fact, they were placed there manually with manipulated file creation dates.

- According to the file listing of a forensically imaged Western Digital hard drive (WD HDD), on 03/30/2009 a backup was made of a Dell Inspiron 700M and given the folder name "BKP.DellInspiron700M-20090330." Also on 03/30/2009 a PowerMac was backed up to the folder "BKP.PowerMac8.2-2009-0330." Unsurprisingly, all the Created dates in these folders were 03/30/2009 (or very early 03/31/2009), the backup date identified in the folder name (see **Appendix A**, Figure 4). By contrast, all the files in the unknown computer ("Dell Dimension") backup folder ("BKP.DellDimension8300-20090330") have a Created date of 07/26/2003, and the backup folder has a last Accessed date of 07/28/2003, despite the folder *name* indicating the same backup date as the others (03/30/2009).
- When files are copied from one file system to another, their Created dates are changed to the current clock time of the machine hosting the receiving file system. If all clocks are accurate, then the created time of these copied files will necessarily be AFTER the modified times.
- In this case, however, all the files in the unknown computer backup ("BKP.DellDimension8300-20090330") have a Created date of 07/26/2003, while most of their Modified dates are from October 2005 and later. This observation indicates the system clock was rolled back to 2003 before copying these files manually onto the hard drive.
- Sometimes the computer's CMOS battery – which enables the computer to retain information after shutdown such as system time – goes bad, resulting in the system clock being reset to a default date, such as 01/01/2003[2]. However, the computer will continue to reset the system clock to that date every time the computer powers up. Therefore, a bad CMOS battery cannot explain the system clock set to 07/26/2003 for the creation date of the files in the folder whose name, as mentioned previously, indicates a 03/30/2009 backup. It also fails to explain the creation dates of several hundred (mostly music) files copied to the WD HDD between 08/08/2003 and 08/18/2003 that were NOT located in the "BACKUPS" folder.
- The rolling back of the system clock is more likely the result of someone who was trying to backdate the folder content and make this folder appear to be a legitimate backup folder but may not have considered how and when file system dates are normally updated.

There are other significant anomalies in this backup folder that showcase the failed effort to create the appearance of an automated backup:

- The Dell Inspiron backup contains more than 15,000 files, while Dell Dimension backup was backed up in two separate copy operations, in total less than 500 files.
- The Dell Inspiron backup included several directories, such as Desktop, Favorites, and My

[2] Although the "factory default" date could theoretically be any date, I have never seen one that is NOT on the first day of the month, either in January or December of the year of manufacture.

Documents, while the Dell Dimension backup initially only included the Studies folder, containing the images in question. It is uncommon for a user to choose to primarily back up a particular folder (in this case, the "Studies" folder) from an entire desktop system, while ignoring more common file storage locations such as My Documents. To accept the legitimacy of this backup one would need to believe a highly improbable scenario where the user made a concerted effort to back up a folder containing his contraband, and specifically this folder, from an entire desktop system. In a likely attempt to create the appearance of a legitimate backup – more than an hour after the "Studies" files were copied – a Symantec folder with one file, and about 150 songs were added to the backup folder.

Conclusion

In summary, the forensic evidence shows that folder names and dates (key facts upon which the prosecution's argument relied) were manually altered, and the entire backup folder to which the alleged contraband belonged was manipulated. While it is impossible to determine exactly when the information on the WD HDD was altered, it is a scientific certainty that data on the CF card were added and/or modified while the device was in FBI custody.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

Appendix A: Figures

Figure 1. CF card file listing showing 9/19/2018 access dates[3].

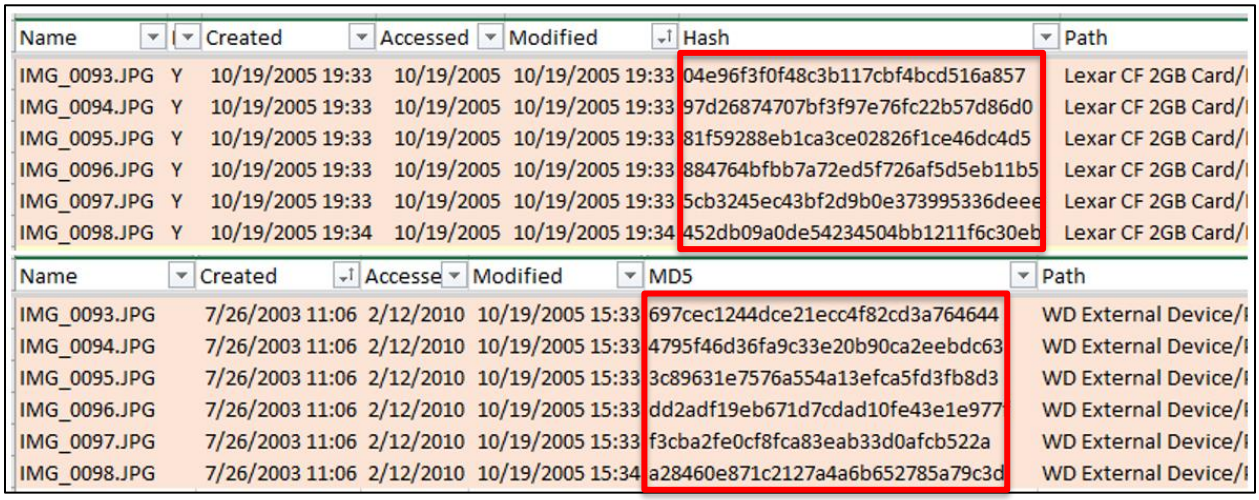
Name	Delete	Created	Accessed	Modified	Hash	Path
IMG_0224.JPG	N	3/9/2006 3:18	9/19/2018	3/9/2006 3:18	596a4251cf7782a440d9b6e8c5c18720	Lexar CF 2GB Card/
IMG_0225.JPG	N	3/9/2006 3:18	9/19/2018	3/9/2006 3:18	1b613027ddb1bafcfcfa88ffd20c6f1e	Lexar CF 2GB Card/
IMG_0227.JPG	N	3/9/2006 3:19	9/19/2018	3/9/2006 3:19	f7ac8c54897985961f729299756fc319	Lexar CF 2GB Card/
IMG_0228.JPG	N	3/9/2006 3:19	9/19/2018	3/9/2006 3:19	341c44c7bd25375f6aeedf39a8db79cc	Lexar CF 2GB Card/
IMG_0229.JPG	N	3/9/2006 3:19	9/19/2018	3/9/2006 3:19	b5ea586450d43d25eda07fffb7f76f82	Lexar CF 2GB Card/
IMG_0230.JPG	N	3/9/2006 3:20	9/19/2018	3/9/2006 3:20	4836010357e1ba89baade965f3d89a0b	Lexar CF 2GB Card/
IMG_0231.JPG	N	3/9/2006 3:20	9/19/2018	3/9/2006 3:20	8bdce71ed54222d649badfcc2d75d898	Lexar CF 2GB Card/
IMG_0233.JPG	N	3/9/2006 3:20	9/19/2018	3/9/2006 3:20	83962b67a98f299f67e6262317c601d5	Lexar CF 2GB Card/
IMG_0234.JPG	N	3/9/2006 3:20	9/19/2018	3/9/2006 3:20	760ac0e77c1d9455c28c07836c52c32b	Lexar CF 2GB Card/
IMG_0235.JPG	N	3/9/2006 3:21	9/19/2018	3/9/2006 3:21	d597dbff4c67fb186b55eff1862e330e	Lexar CF 2GB Card/
IMG_0236.JPG	N	3/9/2006 3:21	9/19/2018	3/9/2006 3:21	534518d5b7cb5e4ab864c04890642294	Lexar CF 2GB Card/
IMG_0237.JPG	N	3/9/2006 3:22	9/19/2018	3/9/2006 3:22	a280f9c541fa96731628987baec67095	Lexar CF 2GB Card/
IMG_0238.JPG	N	3/9/2006 3:22	9/19/2018	3/9/2006 3:22	30788af5673e78bf0365dfb39776d4a9	Lexar CF 2GB Card/
IMG_0239.JPG	N	3/9/2006 3:22	9/19/2018	3/9/2006 3:22	de746ef94d03b6c01797914747cb3601	Lexar CF 2GB Card/
IMG_0241.JPG	N	1/6/2007 7:03	9/19/2018	1/6/2007 7:03	e306c5177fc9cd747dde978233674043	Lexar CF 2GB Card/
IMG_0242.JPG	Y	1/6/2007 7:05	1/6/2007	1/6/2007 7:05	ba9411b3b34b626f73ee4649c757654	Lexar CF 2GB Card/
IMG_0243.JPG	N	1/6/2007 7:05	9/19/2018	1/6/2007 7:05	3b77bc0a1f64652b820d1804b88a8d80	Lexar CF 2GB Card/

Figure 2. Excerpt from DX 945, Chain of Custody for Camera and CF Card, showing SA Lever checking out evidence on 09/19/2018 and returning it on 09/26/2018.

Relinquished Custody	**Date and Time**	**Accepted Custody**	**Date and Time**
Signature: Corey Ellis	9/19/18 0900	Signature:	9/19/18
Printed Name/Agency: Corey Montgomery		Printed Name/Agency: Michael Lever / FBI	
Reason: C/O to SA		Reason: Evidence Review	
Relinquished Custody	**Date and Time**	**Accepted Custody**	**Date and Time**
Signature:	9/26/18 1:15PM	Signature:	9/26/18 1:15PM
Printed Name/Agency: Michael Lever / FBI		Printed Name/Agency:	
Reason: Evidence Return		Reason:	

[3] **Note**: The HDD listing referenced in Figures 1, 3, 4, and 5 was generated by the defense using a computer set to Pacific Time while the government reports were generated by a computer set to Eastern Time.

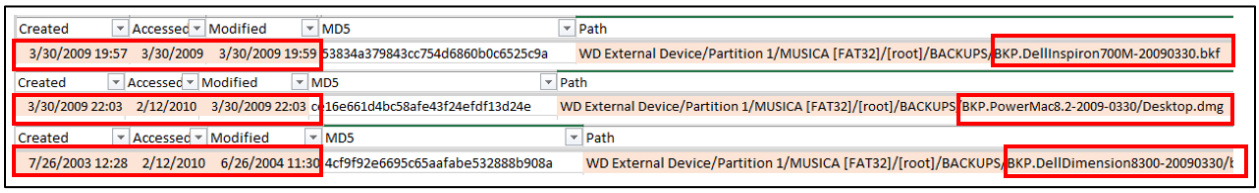
Figure 3. Comparison of photograph metadata for files found on both the CF card and WD HDD.



Name		Created	Accessed	Modified	Hash	Path
IMG_0093.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	04e96f3f0f48c3b117cbf4bcd516a857	Lexar CF 2GB Card/
IMG_0094.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	97d26874707bf3f97e76fc22b57d86d0	Lexar CF 2GB Card/
IMG_0095.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	81f59288eb1ca3ce02826f1ce46dc4d5	Lexar CF 2GB Card/
IMG_0096.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	884764bfbb7a72ed5f726af5d5eb11b5	Lexar CF 2GB Card/
IMG_0097.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	5cb3245ec43bf2d9b0e373995336deee	Lexar CF 2GB Card/
IMG_0098.JPG	Y	10/19/2005 19:34	10/19/2005	10/19/2005 19:34	452db09a0de54234504bb1211f6c30eb	Lexar CF 2GB Card/

Name	Created	Accesse	Modified	MD5	Path
IMG_0093.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	697cec1244dce21ecc4f82cd3a764644	WD External Device/
IMG_0094.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	4795f46d36fa9c33e20b90ca2eebdc63	WD External Device/
IMG_0095.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	3c89631e7576a554a13efca5fd3fb8d3	WD External Device/
IMG_0096.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	dd2adf19eb671d7cdad10fe43e1e977	WD External Device/
IMG_0097.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	f3cba2fe0cf8fca83eab33d0afcb522a	WD External Device/
IMG_0098.JPG	7/26/2003 11:06	2/12/2010	10/19/2005 15:34	a28460e871c2127a4a6b652785a79c3d	WD External Device/

Figure 4. Records from the WD HDD File listing showing disparity in Created dates.



Created	Accessed	Modified	MD5	Path
3/30/2009 19:57	3/30/2009	3/30/2009 19:59	53834a379843cc754d6860b0c6525c9a	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellInspiron700M-20090330.bkf
Created	Accessed	Modified	MD5	Path
3/30/2009 22:03	2/12/2010	3/30/2009 22:03	c16e661d4bc58afe43f24efdf13d24e	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.PowerMac8.2-2009-0330/Desktop.dmg
Created	Accessed	Modified	MD5	Path
7/26/2003 12:28	2/12/2010	6/26/2004 11:30	4cf9f92e6695c65aafabe532888b908a	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/

Figure 5. The WD HDD file listing showing the disparity of parent folders and date/time stamps.

Created	Accesse	Modified	Path
7/26/2003 11:05	2/12/2010	10/19/2005 14:54	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0079.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:54	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0080.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:54	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0081.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:54	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0082.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:55	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0083.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:55	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0084.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:55	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0085.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:55	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0086.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:56	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0087.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:56	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0088.JPG
7/26/2003 11:05	2/12/2010	10/19/2005 14:56	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Msk101905/2005-10-19-0727-59/IMG_0089.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:32	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0090.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:32	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0091.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0092.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0093.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0094.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0095.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0096.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:33	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0097.JPG
7/26/2003 11:06	2/12/2010	10/19/2005 15:34	WD External Device/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/Df101905/2005-10-19-0727-57/IMG_0098.JPG

Figure 6. A comparison of Modified Dates for IMG_0175.JPG, which was modified.

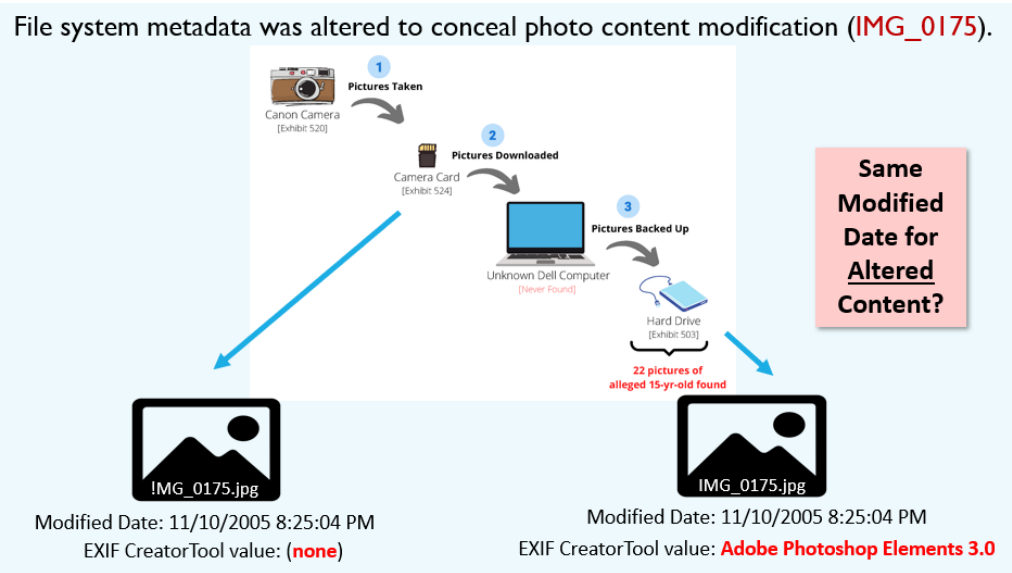
Figure 6a. IMG_0175 file system metadata from the recovered deleted file on the **CF Card** (GX 521 Replacement). This copy could NOT have contained an EXIF CreatorTool value set to "Photoshop Adobe Elements 3.0".

Name !MG_0175.JPG
Extension jpg
Item Number 1064
Path Lexar CF 2GB Card/Partition 1/LEXAR MEDIA [FAT16]/[root]/DCIM/101CANON/!MG_0175.JPG
Created Date 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)
Accessed Date 11/10/2005
Modified Date 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)
MD5 Hash
Deleted True
Carved False

Figure 6b. IMG_0175 file system metadata from the **HDD** (GX 505A). This copy contained EXIF data with a CreatorTool value set to "Photoshop Adobe Elements 3.0".

Name IMG_0175.JPG
Created Date 7/26/2003 2:06:31 PM (2003-07-26 18:06:31 UTC)
Accessed Date 2/12/2010
Modified Date 11/10/2005 8:25:04 PM (2005-11-11 01:25:04 UTC)
MD5 Hash 44725f873418dbf665de0198463f20c9
Path 1B16 WD HD 500GB/Partition 1/MUSICA [FAT32]/[root]/BACKUPS/BKP.DellDimension8300-20090330/Studies/A111005/2005-11-10-0718-42/IMG_0175.JPG
Exported as Report_Files/files/IMG_0175.JPG

Figure 6c. File system metadata was altered to conceal EXIF data modification and support the government's narrative.



Appendix B: File Listing Tables

Table 1: Pictures on hard drive under "Studies" on the hard drive (GX 503)

File Name	WD HDD FAT Modified Date	WD HDD EXIF DateTimeOriginal	Time Shift Between FAT Modified and EXIF DateTimeOriginal (within a few seconds)
IMG_0043.JPG	10/16/05 11:30:04 PM	10/17/05 12:30:04 AM	1
IMG_0044.JPG	10/17/05 3:53:24 PM	10/17/05 4:53:22 PM	1
IMG_0045.JPG	10/17/05 3:53:40 PM	10/17/05 4:53:40 PM	1
IMG_0046.JPG	10/17/05 3:54:08 PM	10/17/05 4:54:09 PM	1
IMG_0047.JPG	10/17/05 3:54:24 PM	10/17/05 4:54:24 PM	1
IMG_0048.JPG	10/17/05 3:54:38 PM	10/17/05 4:54:38 PM	1
IMG_0049.JPG	10/17/05 3:54:54 PM	10/17/05 4:54:54 PM	1
IMG_0050.JPG	10/17/05 3:55:04 PM	10/17/05 4:55:05 PM	1
IMG_0051.JPG	10/17/05 3:55:28 PM	10/17/05 4:55:28 PM	1
IMG_0052.JPG	10/17/05 3:55:42 PM	10/17/05 4:55:41 PM	1
IMG_0053.JPG	10/17/05 3:55:54 PM	10/17/05 4:55:52 PM	1
IMG_0054.JPG	10/17/05 3:55:58 PM	10/17/05 4:55:59 PM	1
IMG_0055.JPG	10/17/05 3:56:24 PM	10/17/05 4:56:25 PM	1
IMG_0056.JPG	10/17/05 3:56:36 PM	10/17/05 4:56:36 PM	1
IMG_0057.JPG	10/17/05 3:56:48 PM	10/17/05 4:56:48 PM	1
IMG_0058.JPG	10/17/05 3:56:58 PM	10/17/05 4:56:58 PM	1
IMG_0059-1.JPG	10/17/05 9:00:58 PM	10/17/05 10:00:57 PM	1
IMG_0060-1.JPG	10/17/05 9:01:06 PM	10/17/05 10:01:07 PM	1
IMG_0061-1.JPG	10/17/05 9:01:12 PM	10/17/05 10:01:13 PM	1
IMG_0062-1.JPG	10/17/05 9:01:24 PM	10/17/05 10:01:24 PM	1
IMG_0063-1.JPG	10/17/05 9:01:32 PM	10/17/05 10:01:32 PM	1
IMG_0064-1.JPG	10/17/05 9:02:00 PM	10/17/05 10:02:00 PM	1

IMG_0065-1.JPG	10/17/05 9:02:08 PM	10/17/05 10:02:07 PM	1
IMG_0066-1.JPG	10/17/05 9:02:14 PM	10/17/05 10:02:13 PM	1
IMG_0067-1.JPG	10/17/05 9:02:34 PM	10/17/05 10:02:34 PM	1
IMG_0068-1.JPG	10/17/05 9:03:02 PM	10/17/05 10:03:01 PM	1
IMG_0069-1.JPG	10/17/05 9:03:10 PM	10/17/05 10:03:10 PM	1
IMG_0070-1.JPG	10/17/05 9:03:24 PM	10/17/05 10:03:24 PM	1
IMG_0071.JPG	10/18/05 7:32:06 PM	10/18/05 8:32:06 PM	1
IMG_0072.JPG	10/18/05 7:32:26 PM	10/18/05 8:32:26 PM	1
IMG_0073.JPG	10/18/05 7:32:36 PM	10/18/05 8:32:36 PM	1
IMG_0074.JPG	10/18/05 7:32:44 PM	10/18/05 8:32:44 PM	1
IMG_0075.JPG	10/18/05 7:33:08 PM	10/18/05 8:33:09 PM	1
IMG_0076.JPG	10/18/05 7:33:14 PM	10/18/05 8:33:15 PM	1
IMG_0077.JPG	10/18/05 7:33:22 PM	10/18/05 8:33:22 PM	1
IMG_0078.JPG	10/18/05 7:33:30 PM	10/18/05 8:33:30 PM	1
IMG_0079.JPG	10/19/05 5:54:08 PM	10/19/05 6:54:09 PM	1
IMG_0080.JPG	10/19/05 5:54:22 PM	10/19/05 6:54:23 PM	1
IMG_0081.JPG	10/19/05 5:54:32 PM	10/19/05 6:54:33 PM	1
IMG_0082.JPG	10/19/05 5:54:56 PM	10/19/05 6:54:57 PM	1
IMG_0083.JPG	10/19/05 5:55:10 PM	10/19/05 6:55:10 PM	1
IMG_0084.JPG	10/19/05 5:55:36 PM	10/19/05 6:55:37 PM	1
IMG_0085.JPG	10/19/05 5:55:48 PM	10/19/05 6:55:49 PM	1
IMG_0086.JPG	10/19/05 5:55:56 PM	10/19/05 6:55:57 PM	1
IMG_0087.JPG	10/19/05 5:56:08 PM	10/19/05 6:56:09 PM	1
IMG_0088.JPG	10/19/05 5:56:24 PM	10/19/05 6:56:24 PM	1
IMG_0089.JPG	10/19/05 5:56:34 PM	10/19/05 6:56:34 PM	1
IMG_0090.JPG	10/19/05 6:32:52 PM	10/19/05 7:32:51 PM	1
IMG_0091.JPG	10/19/05 6:32:58 PM	10/19/05 7:32:57 PM	1

IMG_0092.JPG	10/19/05 6:33:08 PM	10/19/05 7:33:09 PM	1
IMG_0093.JPG	10/19/05 6:33:18 PM	10/19/05 7:33:18 PM	1
IMG_0094.JPG	10/19/05 6:33:26 PM	10/19/05 7:33:25 PM	1
IMG_0095.JPG	10/19/05 6:33:30 PM	10/19/05 7:33:29 PM	1
IMG_0096.JPG	10/19/05 6:33:52 PM	10/19/05 7:33:51 PM	1
IMG_0097.JPG	10/19/05 6:33:58 PM	10/19/05 7:33:57 PM	1
IMG_0098.JPG	10/19/05 6:34:08 PM	10/19/05 7:34:08 PM	1
IMG_0099.JPG	10/20/05 3:20:12 PM	10/20/05 4:20:13 PM	1
IMG_0100.JPG	10/20/05 3:20:30 PM	10/20/05 4:20:31 PM	1
IMG_0101.JPG	10/20/05 3:20:44 PM	10/20/05 4:20:44 PM	1
IMG_0102.JPG	10/20/05 3:21:02 PM	10/20/05 4:21:02 PM	1
IMG_0103.JPG	10/20/05 3:21:28 PM	10/20/05 4:21:28 PM	1
IMG_0104.JPG	10/20/05 3:25:14 PM	10/20/05 4:25:14 PM	1
IMG_0105.JPG	10/20/05 3:26:56 PM	10/20/05 4:26:56 PM	1
IMG_0106.JPG	10/20/05 3:27:04 PM	10/20/05 4:27:03 PM	1
IMG_0107.JPG	10/20/05 3:49:24 PM	10/20/05 4:49:23 PM	1
IMG_0108.JPG	10/20/05 3:49:26 PM	10/20/05 4:49:26 PM	1
IMG_0109.JPG	10/20/05 3:49:30 PM	10/20/05 4:49:29 PM	1
IMG_0110.JPG	10/29/05 4:11:16 AM	10/29/05 5:11:16 AM	1
IMG_0111.JPG	10/29/05 4:11:42 AM	10/29/05 5:11:43 AM	1
IMG_0112.JPG	10/29/05 4:43:36 AM	10/29/05 5:43:36 AM	1
IMG_0113.JPG	10/29/05 4:43:54 AM	10/29/05 5:43:54 AM	1
IMG_0115.JPG	10/29/05 4:44:52 AM	10/29/05 5:44:52 AM	1
IMG_0116.JPG	10/29/05 4:44:56 AM	10/29/05 5:44:55 AM	1
IMG_0117.JPG	10/29/05 4:45:06 AM	10/29/05 5:45:06 AM	1
IMG_0118.JPG	10/29/05 4:45:20 AM	10/29/05 5:45:20 AM	1
IMG_0119.JPG	10/29/05 4:45:26 AM	10/29/05 5:45:25 AM	1

IMG_0120.JPG	10/29/05 4:45:40 AM	10/29/05 5:45:40 AM	1
IMG_0121.JPG	10/29/05 4:45:50 AM	10/29/05 5:45:50 AM	1
IMG_0122.JPG	10/29/05 4:46:00 AM	10/29/05 5:46:00 AM	1
IMG_0123.JPG	10/29/05 4:47:00 AM	10/29/05 5:46:59 AM	1
IMG_0124.JPG	10/29/05 4:47:06 AM	10/29/05 5:47:05 AM	1
IMG_0125.JPG	10/29/05 4:47:10 AM	10/29/05 5:47:11 AM	1
IMG_0126.JPG	10/29/05 4:47:24 AM	10/29/05 5:47:24 AM	1
IMG_0127.JPG	10/30/05 2:34:20 AM	10/30/05 4:34:20 AM	2
IMG_0128.JPG	10/30/05 2:35:14 AM	10/30/05 4:35:14 AM	2
IMG_0129.JPG	10/30/05 2:36:06 AM	10/30/05 4:36:05 AM	2
IMG_0130.JPG	10/30/05 2:36:42 AM	10/30/05 4:36:42 AM	2
IMG_0131.JPG	10/30/05 2:36:54 AM	10/30/05 4:36:55 AM	2
IMG_0132.JPG	10/30/05 2:37:12 AM	10/30/05 4:37:12 AM	2
IMG_0133.JPG	10/30/05 2:37:44 AM	10/30/05 4:37:45 AM	2
IMG_0134.JPG	10/30/05 2:37:58 AM	10/30/05 4:37:58 AM	2
IMG_0135.JPG	10/30/05 2:38:00 AM	10/30/05 4:38:00 AM	2
IMG_0136.JPG	10/30/05 3:39:00 AM	10/30/05 5:39:00 AM	2
IMG_0137.JPG	10/30/05 3:39:06 AM	10/30/05 5:39:06 AM	2
IMG_0138.JPG	10/30/05 4:55:42 PM	10/30/05 4:55:41 PM	0
IMG_0139.JPG	10/30/05 4:55:52 PM	10/30/05 4:55:51 PM	0
IMG_0140.JPG	10/30/05 4:56:20 PM	10/30/05 4:56:21 PM	0
IMG_0141.JPG	10/30/05 4:56:46 PM	10/30/05 4:56:46 PM	0
IMG_0142.JPG	10/30/05 4:57:12 PM	10/30/05 4:57:12 PM	0
IMG_0143.JPG	10/30/05 6:01:08 PM	10/30/05 6:01:08 PM	0
IMG_0144.JPG	10/30/05 6:01:14 PM	10/30/05 6:01:14 PM	0
IMG_0145.JPG	10/30/05 6:01:20 PM	10/30/05 6:01:19 PM	0
IMG_0146.JPG	10/30/05 6:01:28 PM	10/30/05 6:01:28 PM	0

IMG_0147.JPG	10/30/05 6:02:08 PM	10/30/05 6:02:08 PM	0
IMG_0148.JPG	10/30/05 6:02:14 PM	10/30/05 6:02:15 PM	0
IMG_0149.JPG	10/30/05 6:02:22 PM	10/30/05 6:02:22 PM	0
IMG_0150.JPG	11/2/05 5:59:16 PM	11/02/05 5:59:16 PM	0
IMG_0151.JPG	11/2/05 5:59:26 PM	11/02/05 5:59:25 PM	0
IMG_0152.JPG	11/2/05 5:59:30 PM	11/02/05 5:59:30 PM	0
IMG_0153.JPG	11/2/05 5:59:34 PM	11/02/05 5:59:34 PM	0
IMG_0154.JPG	11/2/05 5:59:48 PM	11/02/05 5:59:47 PM	0
IMG_0155.JPG	11/2/05 6:00:22 PM	11/02/05 6:00:22 PM	0
IMG_0156.JPG	11/2/05 6:00:30 PM	11/02/05 6:00:29 PM	0
IMG_0157.JPG	11/2/05 6:00:38 PM	11/02/05 6:00:38 PM	0
IMG_0158.JPG	11/2/05 6:00:48 PM	11/02/05 6:00:49 PM	0
IMG_0159.JPG	11/2/05 6:01:10 PM	11/02/05 6:01:10 PM	0
IMG_0160.JPG	11/2/05 6:01:18 PM	11/02/05 6:01:18 PM	0
IMG_0161.JPG	11/2/05 6:09:00 PM	11/02/05 6:08:59 PM	0
IMG_0162.JPG	11/2/05 6:09:02 PM	11/02/05 6:09:02 PM	0
IMG_0163.JPG	11/2/05 6:09:10 PM	11/02/05 6:09:11 PM	0
IMG_0164.JPG	11/10/05 8:22:18 PM	11/10/05 8:22:18 PM	0
IMG_0165.JPG	11/10/05 8:22:30 PM	11/10/05 8:22:30 PM	0
IMG_0168.JPG	11/10/05 8:23:12 PM	11/10/05 8:23:12 PM	0
IMG_0169.JPG	11/10/05 8:23:26 PM	11/10/05 8:23:26 PM	0
IMG_0172.JPG	11/10/05 8:24:20 PM	11/10/05 8:24:19 PM	0
IMG_0174.JPG	11/10/05 8:24:48 PM	11/10/05 8:24:47 PM	0
IMG_0175.JPG	11/10/05 8:25:04 PM	11/10/05 8:25:04 PM	0
IMG_0176.JPG	11/10/05 8:25:10 PM	11/10/05 8:25:11 PM	0
IMG_0177.JPG	11/10/05 8:25:36 PM	11/10/05 8:25:35 PM	0
IMG_0178.JPG	11/10/05 8:25:54 PM	11/10/05 8:25:54 PM	0

IMG_0179.JPG	11/10/05 8:26:04 PM	11/10/05 8:26:04 PM	0
IMG_0180.JPG	11/10/05 8:26:22 PM	11/10/05 8:26:22 PM	0
IMG_0181.JPG	11/10/05 8:26:26 PM	11/10/05 8:26:25 PM	0
IMG_0182.JPG	11/10/05 8:26:30 PM	11/10/05 8:26:29 PM	0
IMG_0183.JPG	11/10/05 8:27:34 PM	11/10/05 8:27:33 PM	0
IMG_0184.JPG	11/24/05 9:07:50 PM	11/24/05 9:07:50 PM	0
IMG_0185.JPG	11/24/05 9:07:56 PM	11/24/05 9:07:55 PM	0
IMG_0186.JPG	11/24/05 9:08:08 PM	11/24/05 9:08:07 PM	0
IMG_0187.JPG	11/24/05 9:09:52 PM	11/24/05 9:09:52 PM	0
IMG_0188.JPG	11/24/05 9:10:08 PM	11/24/05 9:10:08 PM	0
IMG_0189.JPG	11/24/05 9:10:22 PM	11/24/05 9:10:23 PM	0
IMG_0190.JPG	11/24/05 9:10:28 PM	11/24/05 9:10:28 PM	0
IMG_0191.JPG	11/24/05 9:10:38 PM	11/24/05 9:10:37 PM	0
IMG_0194.JPG	12/18/05 12:37:58 AM	12/18/05 12:37:58 AM	0
IMG_0197.JPG	12/18/05 12:38:20 AM	12/18/05 12:38:20 AM	0
IMG_0198.JPG	12/18/05 12:38:28 AM	12/18/05 12:38:28 AM	0
IMG_0199.JPG	12/18/05 12:38:56 AM	12/18/05 12:38:55 AM	0
IMG_0203.JPG	12/25/05 2:59:44 AM	12/25/05 2:59:44 AM	0
IMG_0204.JPG	12/25/05 2:59:50 AM	12/25/05 2:59:50 AM	0
IMG_0205.JPG	12/25/05 3:00:42 AM	12/25/05 3:00:42 AM	0
IMG_0206.JPG	12/25/05 3:00:50 AM	12/25/05 3:00:49 AM	0
IMG_0207.JPG	12/25/05 3:01:40 AM	12/25/05 3:01:40 AM	0
IMG_0208.JPG	12/25/05 3:01:46 AM	12/25/05 3:01:46 AM	0
IMG_0209.JPG	12/30/05 5:56:06 PM	12/30/05 5:56:05 PM	0
IMG_0210.JPG	12/30/05 5:56:12 PM	12/30/05 5:56:11 PM	0
IMG_0211.JPG	12/30/05 5:56:16 PM	12/30/05 5:56:15 PM	0
IMG_0212.JPG	12/30/05 5:56:20 PM	12/30/05 5:56:20 PM	0

IMG_0213.JPG	12/30/05 5:56:46 PM	12/30/05 5:56:46 PM	0
IMG_0214.JPG	12/30/05 5:56:54 PM	12/30/05 5:56:53 PM	0
IMG_0215.JPG	12/30/05 5:56:56 PM	12/30/05 5:56:56 PM	0
IMG_0216.JPG	12/30/05 5:57:00 PM	12/30/05 5:56:59 PM	0
IMG_0217.JPG	12/30/05 5:58:50 PM	12/30/05 5:58:50 PM	0
IMG_0218.JPG	12/30/05 5:59:00 PM	12/30/05 5:58:59 PM	0
IMG_0219.JPG	12/30/05 5:59:08 PM	12/30/05 5:59:07 PM	0
IMG_0220.JPG	12/30/05 5:59:18 PM	12/30/05 5:59:18 PM	0
IMG_0221.JPG	12/30/05 5:59:56 PM	12/30/05 5:59:56 PM	0
IMG_0222.JPG	12/30/05 6:00:08 PM	12/30/05 6:00:08 PM	0
IMG_0223.JPG	12/30/05 6:00:24 PM	12/30/05 6:00:24 PM	0

Appendix C: Analysis of Files Carved from HDD and CF Card

The content of four digital photos, IMG_0180 through IMG_0183, are the only ones that are exactly the same across both the CF card (GX 521A) and the external hard drive (GX 503), meaning they are the only photos whose file names and MD5 hashes match. Initially, this was discovered by comparing the file hashes from two file listings, "CF card listing.csv" and "File Listing of Backup Folder (BKP.DellDimension8300-20090330).csv," derived from the FBI's FTK reports.

In addition, I inspected two additional file listings, "GX 521A Replacement (carved files)_2019_06_11.csv" and "Full File Listing of Hard Drive Contents (GX 503).csv," which provided items *carved* from the CF card and external hard drive, respectively. In these listings I discovered a suspicious relationship between photos IMG_0180 through IMG_0183 and four other photos on the CF card, IMG_0093, IMG_0094, IMG_0096, and IMG_0097, respectively.

Before I describe those relationships, however, it would be helpful for the reader to understand how carved files are generated. Figure 1 represents a digital photograph named **IMG_0180.JPG**, which has a file size of 2,539,833 bytes (about 2.5 MB). The logical portion of the file consists of three primary components.

- **EXIF data**, which typically contains camera-generated metadata, is fixed length and occupies the first portion of the file from byte offset 0 to offset 9728.
- The second portion of the file is the picture **thumbnail**, a variable-length component that occupies the space between the end of the EXIF data (offset 9728) and the beginning of the main picture (offset 16845). Subtracting these two numbers provides the file size of the thumbnail, 7,117 bytes. When a forensic tool carves it from the parent file it is given the file name "Carved [9728].jpeg," indicating its starting location in the file.
- The third portion of the file is the **main picture**, occupying the largest portion of the file at 2,522,988 bytes. Since the main picture begins at byte offset 16845, the carving forensic tool will give it a file name of "Carved [16845].jpeg."

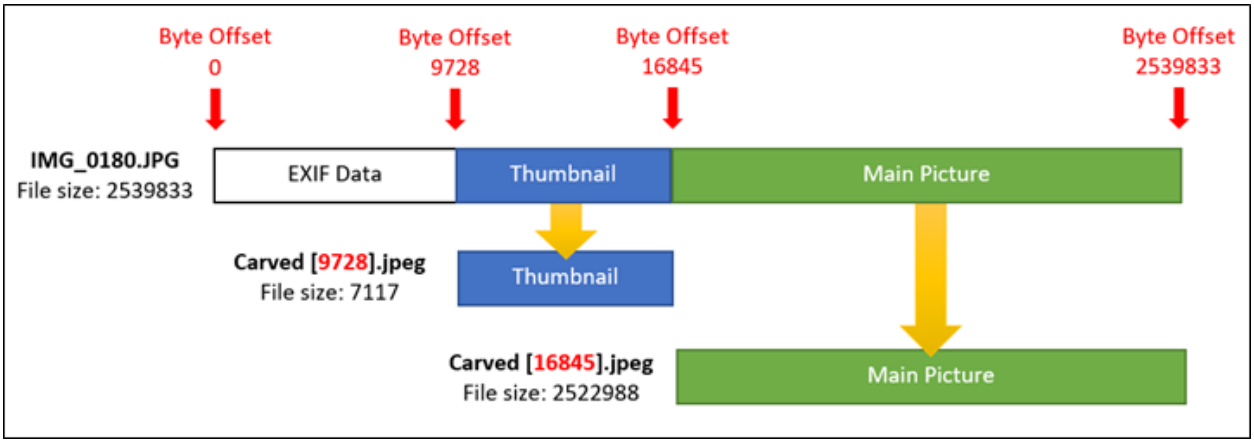


Figure 1. How a forensic tool creates and names files carved from digital photographs.

For brevity I will limit the discussion of the suspicious files (IMG_0093, IMG_0094, IMG_0096, and IMG_0097) to the relationship between IMG_0093 and IMG_0180. The corresponding relationships between IMG_0094, IMG_0096, IMG_0097 and IMG_181, IMG_182, IMG_183, respectively, are identical.

Table 1 below was excerpted from "Full File Listing of Hard Drive Contents (GX 503).csv" and displays information about IMG_0093 and IMG_0180. As discussed elsewhere, the Created dates do not make sense. That anomaly aside, however, the file size information is consistent. For example, for each file the logical size (L-Size) added to the size of its corresponding FileSlack is equal to the physical size (P-size), as it should. Also, each of these files have corresponding carved files, including "Carved [9728].jpeg," which is a thumbnail picture carved starting at byte offset 9728. With a single exception - as explained previously - the thumbnail files for each digital photograph in this case can be identified by the name "Carved [9728].jpeg." A second carved file, "Carved [XXXXX].jpeg," which is the main picture carved starting at byte offset XXXXX, will vary with each photo because thumbnail sizes are different. The table below demonstrates that subtracting the two starting byte offsets for the carved files (in **red**) predictably results in the logical size for the thumbnail (in **blue**).

Row	Name	Category	Created	Accessed	Modified	P-Size (bytes)	L-Size (bytes)	MD5
1	**IMG_0093.JPG**	JPEG EXIF	7/26/2003 11:06	2/12/2010	10/19/2005 15:33	2523136	2500404	697cec1244dce21ecc4f82cd3a764644
2	IMG_0093.JPG.File Slack	Slack Space	n/a	n/a	n/a	22732	22732	
3	Carved [**14844**].jpeg	JPEG	n/a	n/a	n/a	n/a	2485560	ae6cbe511c9f3bdec52917e3dca05129
4	Carved [**9728**].jpeg	JPEG	n/a	n/a	n/a	n/a	**5116**	51202a6c4b8e6084f15345656156481c
5	**IMG_0180.JPG**	JPEG EXIF	7/26/2003 11:06	2/12/2010	11/10/2005 17:26	2555904	2539833	f6202d0b41e30c7c21aeae32c38baf9b
6	IMG_0180.JPG.File Slack	Slack Space	n/a	n/a	n/a	16071	16071	
7	Carved [**16845**].jpeg	JPEG	n/a	n/a	n/a	n/a	2522988	b991eaa84b4d91dfa2d0eece1e902430
8	Carved [**9728**].jpeg	JPEG	n/a	n/a	n/a	n/a	**7117**	6babe3f7c2bd2c6c73d15e3d2db42a95

Table 1. Excerpt from "Full File Listing of Hard Drive Contents (GX 503).csv."

Next we turn our attention to an excerpt from "GX 521A Replacement (carved files)_2019_06_11.csv," which also displays information about IMG_0093 and IMG_0180 - but on the CF card. There are several inconsistencies with this data (See Table 2).

- The file named "Carved [2129920].jpeg" indicates the file was carved from **IMG_0093** starting at byte offset 2129920. This would mean the file would have been carved starting near the *end* of the digital photo file, which has a logical size of 2500404 bytes according to the previous table. There was no file size data present in this file listing (which is suspicious in itself). However, subtracting 2129920 from 2500404 yields a maximum file size of 370484 bytes for this carved file, which is too large to be a thumbnail and too small to be the main picture data for the photo.
- In row 2 a file named "Carved [16845].jpeg" indicates the file was carved from "Carved [2129920].jpeg" (which was itself carved from IMG_0093) starting at byte offset 16845. Surprisingly, this is **precisely the same byte offset** that began the main picture carving in **IMG_0180** as shown in this table (row 5) and verified in the previous table by a matching MD5 hash (See Table 1, row 7).
- As discussed earlier, files in this case named "Carved [9728].jpeg" are thumbnails that are carved from their parent photo files starting at byte offset 9728. However, the **same thumbnail** (with matching hashes) was **carved from two different files**, **IMG_0093** and **IMG_0180**. (See Table 2, rows 3-4 and compare at Table 1, row 8).

Row	Path	Hash	Name	Deleted?
1	/DCIM/100CANON/**! MG_0093.JPG**»Carved [2129920].jpeg	8514c14257901fca23dab82db71f6c0c	! MG_0093.JPG»Carved [2129920].jpeg	Y
2	/DCIM/100CANON/**! MG_0093.JPG**»Carved [2129920].jpeg»Carved [**16845**].jpeg	d4831cccb7f5ac74632cc09a32d28515	! MG_0093.JPG»Carved [2129920].jpeg»Carved [16845].jpeg	Y
3	/DCIM/100CANON/**! MG_0093.JPG**»Carved [2129920].jpeg»Carved [**9728**].jpeg	6babe3f7c2bd2c6c73d15e3d2db42a95	! MG_0093.JPG»Carved [2129920].jpeg»Carved [9728].jpeg	Y
4	/DCIM/101CANON/**! MG_0180.JPG**»Carved [**9728**].jpeg	6babe3f7c2bd2c6c73d15e3d2db42a95	! MG_0180.JPG»Carved [9728].jpeg	Y
5	/DCIM/101CANON/! MG_0180.JPG»Carved [**16845**].jpeg	b991eaa84b4d91dfa2d0eece1e902430	! MG_0180.JPG»Carved [16845].jpeg	Y

Table 2. Excerpt from "GX 521A Replacement (carved files)_2019_06_11.csv" (second listing for the CF card, with no file sizes present).

As mentioned previously, the same pattern appears in the file listings for relationships between IMG_0094 and IMG_0181, IMG_0096 and IMG_0182, and IMG_0097 and IMG_0183. Two additional observations point to IMG_0093, IMG_0094, IMG_0096, and IMG_0097 being counterfeit files on the CF card:

- With the exception of unallocated space, the files IMG_0093, IMG_0094, IMG_0096, and IMG_0097 are the only files in the CF card file listing with apparent nested carving (carving from carved files).
- Unlike the consistency of files IMG_0180 to IMG_0183, the byte offset data and MD5 hashes of files IMG_0093, IMG_0094, IMG_0096, and IMG_0097 are NOT consistent between Tables 1 and 2 (i.e., between the hard drive and CF card).

Other anomalous behavior

Additional analyses of the CF card and WD HDD file listings reveal bizarre patterns that support the finding that files were altered and transferred between devices:

- A group of files located on the WD HDD were given **nonstandard file names**, from IMG_0059-1 to IMG_0070-1. Neither the 04/11/2019 nor the 06/11/2019 CF card file listings contain any record of these photos existing on the CF card, despite their camera-related EXIF data being identical to all the others. Notably, these names were not assigned automatically by the camera, but were rather created by a user action, thus proving at least one aspect of metadata editing.
- The CF card file listing shows large swaths of missing file name sequences, and sequences with no content, punctuated by groups of 5-6 files with recoverable content (see Table 3). This is not consistent with normal use of a camera, where the user might review and choose to occasionally delete unwanted photographs as desired. Rarely would this deletion activity follow such a distinctive pattern as what appears in the file listing. However, the pattern would be consistent with someone copying photos between the CF card and an unknown computer.

Name	Delete	Created	Accessed	Modified	Hash	Path
IMG_0089.JPG	Y	10/19/2005 18:56	10/19/2005	10/19/2005 18:56	NO HASH	Lexar CF 2GB Card/
IMG_0090.JPG	Y	10/19/2005 19:32	10/19/2005	10/19/2005 19:32	NO HASH	Lexar CF 2GB Card/
IMG_0091.JPG	Y	10/19/2005 19:32	10/19/2005	10/19/2005 19:32	NO HASH	Lexar CF 2GB Card/
IMG_0092.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	NO HASH	Lexar CF 2GB Card/
IMG_0093.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	04e96f3f0f48c3b117cbf4bcd516a857	Lexar CF 2GB Card/
IMG_0094.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	97d26874707bf3f97e76fc22b57d86d0	Lexar CF 2GB Card/
IMG_0095.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	81f59288eb1ca3ce02826f1ce46dc4d5	Lexar CF 2GB Card/
IMG_0096.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	884764bfbb7a72ed5f726af5d5eb11b5	Lexar CF 2GB Card/
IMG_0097.JPG	Y	10/19/2005 19:33	10/19/2005	10/19/2005 19:33	5cb3245ec43bf2d9b0e373995336deee	Lexar CF 2GB Card/
IMG_0098.JPG	Y	10/19/2005 19:34	10/19/2005	10/19/2005 19:34	452db09a0de54234504bb1211f6c30eb	Lexar CF 2GB Card/
IMG_0099.JPG	Y	10/20/2005 16:20	10/20/2005	10/20/2005 16:20	NO HASH	Lexar CF 2GB Card/
IMG_0100.JPG	Y	10/20/2005 16:20	10/20/2005	10/20/2005 16:20	NO HASH	Lexar CF 2GB Card/
GAP - Alleged contraband images 0150-0163 do not appear here at all						
IMG_0172.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24	NO HASH	Lexar CF 2GB Card/
IMG_0173.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24	NO HASH	Lexar CF 2GB Card/
IMG_0174.JPG	Y	11/10/2005 20:24	11/10/2005	11/10/2005 20:24	NO HASH	Lexar CF 2GB Card/
IMG_0175.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25	NO HASH	Lexar CF 2GB Card/
IMG_0176.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25	NO HASH	Lexar CF 2GB Card/
IMG_0177.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25	NO HASH	Lexar CF 2GB Card/
IMG_0178.JPG	Y	11/10/2005 20:25	11/10/2005	11/10/2005 20:25	NO HASH	Lexar CF 2GB Card/
IMG_0179.JPG	Y	11/10/2005 20:26	11/10/2005	11/10/2005 20:26	ab069f934603db10d2b579a5323a117c	Lexar CF 2GB Card/
IMG_0180.JPG	Y	11/10/2005 20:26	11/10/2005	11/10/2005 20:26	f6202d0b41e30c7c21aeae32c38baf9b	Lexar CF 2GB Card/
IMG_0181.JPG	Y	11/10/2005 20:26	11/10/2005	11/10/2005 20:26	c22d37f14011b042388917706a89c4a9	Lexar CF 2GB Card/
IMG_0182.JPG	Y	11/10/2005 20:26	11/10/2005	11/10/2005 20:26	550df2c454f2c70cc0911f6ceaad4549	Lexar CF 2GB Card/
IMG_0183.JPG	Y	11/10/2005 20:27	11/10/2005	11/10/2005 20:27	b0d057b32850bfc7c20674f7dfa1ae3a	Lexar CF 2GB Card/
GAP - Alleged contraband images 0184-0191 do not appear here at all						
IMG_0193.JPG	Y	12/19/2005 0:37	12/19/2005	12/19/2005 0:37	NO HASH	Lexar CF 2GB Card/

Table 3. Analysis showing conspicuous gaps in data appearing in the CF card file listing.

Summary

According to the file paths and hash values I observed, the carving byte offset data and thumbnails are exactly the same in two sets of files purported to be different. To be clear, two different digital photographs would *never* share exactly the same thumbnail picture. It is impossible without manual intervention. Moreover, the photographs IMG_0093, IMG_0094, IMG_0096, and IMG_0097, produced multiple, duplicate carved files, which on flash media is indicative of file modification. By contrast, all the other files on the CF card file listing contain exactly two carved files: a thumbnail named "Carved [9728].jpeg" and a carved main picture named "Carved [XXXXX].jpeg."

Given the above facts, I believe the following actions describe the most plausible explanation for what I observed with regard to the eight files in question.

These four files (IMG_0180 through IMG_0183) were either manually copied from an unknown computer to the CF card or else were copied from the CF card to the unknown computer, where they were "backed up" to the external hard drive. This action would explain the fact that these four files (the only four of about 200) actually matched hashes between devices. Also, it is likely that someone copied another version of these *same four files* to the CF card, altered their content, and renamed them to IMG_0093, IMG_0094, IMG_0096, and IMG_0097. These actions would

explain 1) why these files bear no resemblance to those on the hard drive with the same file names, 2) why they contain the identical thumbnail pictures and common starting byte offsets as those contained in the IMG_0180 to IMG_0183 files, 3) why there are multiple, carved instances of these files on the flash media, and 4) why none of these files appeared on the 04/11/2019 CF card file listing while appearing on the subsequent 06/11/2019 file listing. There are no plausible natural or automated causes to explain such phenomena.

In summary, the forensic evidence demonstrates that alterations were intentionally made to files on the CF card, and the differences between the 04/11/2019 and 06/11/2019 file listings suggest those alterations took place while the CF card was in the custody of the FBI, as the devices were collected on March 27, 2018.

Appendix D: Description of New Files Appearing on the FBI's Forensic Report Between 04/11/2019 and 06/11/2019

By J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

Introduction:

In the present case, U.S. vs KEITH RANIERE, the FBI completed two forensic examinations and generated two different reports on the same piece of evidence: A compact flash (CF) card found in a digital camera case. The Government claimed that digital photographs from this CF Card were eventually backed up to a Western Digital hard disk drive (WD HDD), which also contained alleged child pornography. The government's narrative depended on creating a strong connection between the CF Card, allegedly belonging to the defendant, and the WD HDD that supposedly backed up photos from the CF Card. This brief analysis offers a plausible explanation for why a second examination, and a second report of the CF Card, were generated by an FBI forensic examiner (FE)[1].

Figure 1: Files Appearing on the First FBI Forensic Reports of the CF Card and WD HDD

04/11/2019 CF Card Report 	**04/11/2019** WD HDD Report 
IMG_0021-41	
	IMG_0043-79
	IMG_0081-100
	IMG_0101-149
	IMG_0150-163
	IMG_0164,5,8,9
	IMG_0172-79 sans 173
IMG_0180-183	IMG_0180-183
	IMG_0184-191
	IMG_0194,7,8,9
	IMG_0203-223
IMG_0224-0243, sans 0226, 0232, and 0240	

Photo range of alleged contraband – not included in WD HDD report.

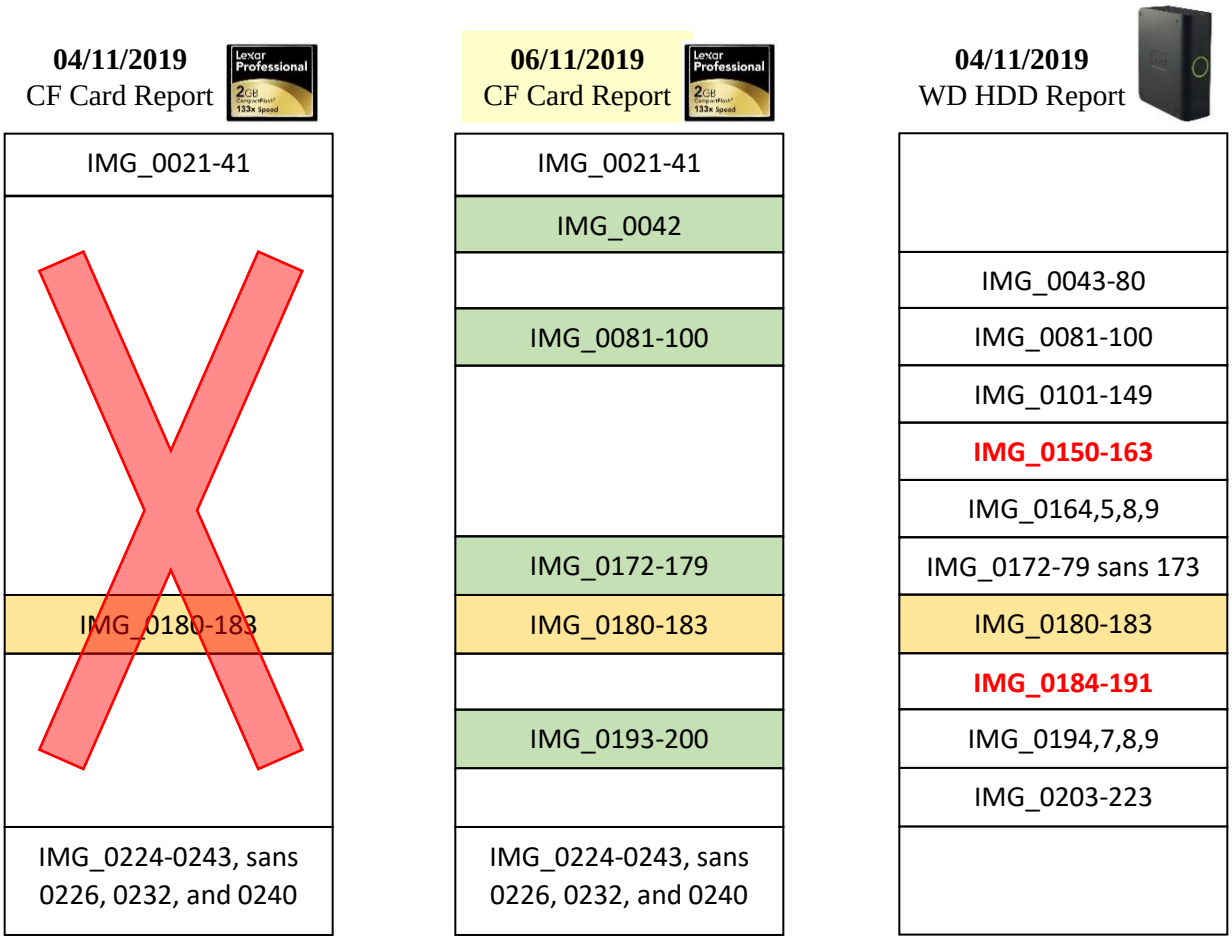
Photo range of alleged contraband – not included in WD HDD report.

Observations:

- Both forensic reports were generated on the same day, **April 11, 2019**.
- The **CF Card report** was created by **FE Stephen Flatley**, who kept the CF Card until 06/07/2022.
- The **WD HDD report** was created by **FE Brian Booth**, using a forensic copy made by his trainee.
- Only **four photos**, named IMG_0180-183, are common to both forensic reports (highlighted yellow).
- At this time **no other files** on the CF Card report could be shown to be "backed up" to the WD HDD.

[1] For more information about the background of the case and the Government's narrative presented at trial, please see my full reports detailing Technical and Process Findings.

Figure 2: Generating the Second FBI Forensic Report on the CF Card (June 11, 2019)



Observations:

- As documented in the Chain of Custody, SA Mills delivered the CF Card, in an **unsealed bag**, to FE Booth on 06/10/2019, during the last week of trial and more than **14 months** after the search team had collected it.
- SA Lever requested that FE Booth complete a **new examination** and a **new "replacement" report** (dated 06/11/2019 in the above figure).
- **None** of the new files appearing on the 06/11/2019 report (shaded green) was viewable in the report.
- No explanation was provided for the appearance of the new files or why they were **unviewable**.
- **All** the previous CF Card files (in white) are viewable in both CF Card reports.
- It is extremely unlikely that **eight of the new files** on the 6/11 CF Card report (IMG_0172-179) just happen to occupy the filename space before the small group of "common" photos (IMG_0180-183) and then **another eight new files** (IMG_0193-200) just happen to appear right after the alleged contraband photo range (IMG_0184-191), which themselves just happen to appear immediately after the common photos.
- The **alleged contraband** photos, IMG_0150-163 and IMG_0184-191, appear in neither of the CF Card reports. If the government's narrative was correct, then one would reasonably expect some remnants of these photos to have been included on the FBI's reports.
- IMG_0042 appears **only** on the 6/11 CF Card report – so it seems to fill a filename "gap."
    - IMG_0021-0041 appear on the 4/11 CF Card report but not on the WD HDD report.
    - IMG_0043-0179 appear on the WD HDD report but not on the 4/11 CF Card report.
- The new file ranges on the 6/11 report are **uninterrupted**. Unlike the WD HDD report, there are no missing file names or gaps within each group of new files.

Figure 3: Evidence Supporting the Addition of New Files to the CF Card

IMG_0079.JPG	10/19/05 2:54 PM	/Msk101905/2005-10-19-0727-59/IMG_0079.JPG
IMG_0080.JPG	10/19/05 2:54 PM	/Msk101905/2005-10-19-0727-59/IMG_0080.JPG
IMG_0081.JPG	10/19/05 2:54 PM	/Msk101905/2005-10-19-0727-59/IMG_0081.JPG
IMG_0082.JPG	10/19/05 2:54 PM	/Msk101905/2005-10-19-0727-59/IMG_0082.JPG
IMG_0083.JPG	10/19/05 2:55 PM	/Msk101905/2005-10-19-0727-59/IMG_0083.JPG
IMG_0084.JPG	10/19/05 2:55 PM	/Msk101905/2005-10-19-0727-59/IMG_0084.JPG
IMG_0085.JPG	10/19/05 2:55 PM	/Msk101905/2005-10-19-0727-59/IMG_0085.JPG
IMG_0086.JPG	10/19/05 2:55 PM	/Msk101905/2005-10-19-0727-59/IMG_0086.JPG
IMG_0087.JPG	10/19/05 2:56 PM	/Msk101905/2005-10-19-0727-59/IMG_0087.JPG
IMG_0088.JPG	10/19/05 2:56 PM	/Msk101905/2005-10-19-0727-59/IMG_0088.JPG
IMG_0089.JPG	10/19/05 2:56 PM	/Msk101905/2005-10-19-0727-59/IMG_0089.JPG
IMG_0090.JPG	10/19/05 3:32 PM	/Df101905/2005-10-19-0727-57/IMG_0090.JPG
IMG_0091.JPG	10/19/05 3:32 PM	/Df101905/2005-10-19-0727-57/IMG_0091.JPG
IMG_0092.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0092.JPG
IMG_0093.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0093.JPG
IMG_0094.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0094.JPG
IMG_0095.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0095.JPG
IMG_0096.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0096.JPG
IMG_0097.JPG	10/19/05 3:33 PM	/Df101905/2005-10-19-0727-57/IMG_0097.JPG
IMG_0098.JPG	10/19/05 3:34 PM	/Df101905/2005-10-19-0727-57/IMG_0098.JPG
IMG_0099.JPG	10/20/05 12:20 PM	/Mnp102005/2005-10-20-0640-31/IMG_0099.JPG
IMG_0100.JPG	10/20/05 12:20 PM	/Mnp102005/2005-10-20-0640-31/IMG_0100.JPG
IMG_0101.JPG	10/20/05 12:20 PM	/Mnp102005/2005-10-20-0640-31/IMG_0101.JPG
IMG_0102.JPG	10/20/05 12:21 PM	/Mnp102005/2005-10-20-0640-31/IMG_0102.JPG
IMG_0103.JPG	10/20/05 12:21 PM	/Mnp102005/2005-10-20-0640-31/IMG_0103.JPG
IMG_0104.JPG	10/20/05 12:25 PM	/Mnp102005/2005-10-20-0640-31/IMG_0104.JPG
IMG_0105.JPG	10/20/05 12:26 PM	/Mnp102005/2005-10-20-0640-31/IMG_0105.JPG
IMG_0106.JPG	10/20/05 12:27 PM	/Mnp102005/2005-10-20-0640-31/IMG_0106.JPG
IMG_0107.JPG	10/20/05 12:49 PM	/Mnp102005/2005-10-20-0640-31/IMG_0107.JPG
IMG_0108.JPG	10/20/05 12:49 PM	/Mnp102005/2005-10-20-0640-31/IMG_0108.JPG

Why were **only the last nine photos** (not the first two) from **Msk101905** added to the new 6/11 CF Card Report?

Photo files shaded in green were added to the **06/11** CF Card report and did not appear on the **4/11** report.

Why were **only the first two photos** (not the last eight) from **Mnp102005** added to the new 6/11 CF Card Report?

Observations:

- The above file listing was adapted from the WD HDD report, so **all** these files appear in the "backup" drive.
- **None** of these files appear on the 4/11 CF Card report.
- Files shaded in **green** appear on the 6/11 CF Card report, but none of them are viewable on that report.
- Files with a **red** boundary were located in the WD HDD's Msk101905 folder.
- Files with a **blue** boundary were located in the WD HDD's Mnp102005 folder.
- It is **extremely unlikely** that photos would have been saved to and deleted from the CF Card in this manner as a result of normal user behavior (See Implications discussion below).

Implications

As explained elsewhere, the Government claimed that digital photos, including **alleged contraband**, had been created with a Canon camera, saved to the camera's CF card, transferred to an unknown computer, and then backed up to the WD HDD. **Figure 1** illustrates the initially weak relationship between files on the CF card and the alleged "backup" of those files contained in the WD HDD. In fact, according to the FBI's report on 04/11/2019, **only four photographs** were reported as being common to both devices.

In **Figure 2**, however, the introduction of **new files** to the FBI's 06/11/2019 "replacement" forensic report creates an obviously stronger relationship between the devices. In all, 37 photos with filenames matching those on the WD HDD were added to the 06/11/2019 report in small, contiguous groups of files. Unfortunately – or perhaps, *conveniently* – **none of the new files were viewable** as photographs in the second report. As a result, none of the new files could be verified visually or forensically against their namesakes on the WD HDD report.[2] The FBI never provided an explanation for the appearance of new photos on the 06/11/2019 report or why they were the only photos on the CF card that were not viewable in the report.

Figure 3 requires a more robust explanation. In the case of the new files **IMG_0081-100** (highlighted in green), it seems that someone decided to **add the appearance of those 20 files** using round start and end **file numbers** – but without regard for the three separate **folders** into which their namesakes would eventually be discovered on the WD HDD "backup." To accept the integrity and completeness of the 6/11 CF Card report, one must believe that the user:

- Took photos IMG_0079-89 on the CF Card,
- Saved the eleven photos to the Msk101905/2005-10-19-0727-59 folder on the unknown computer,
- Returned to the CF Card and *securely* deleted[3] the only the first two photos in that series (IMG_0079-80),
- Took photos IMG_0099-108 on the CF Card,
- Saved the ten photos to the /Mnp102005/2005-10-20-0640-31 folder on the unknown computer, and
- Returned to the CF Card and *securely* deleted **all BUT** the first two photos in the series (IMG_0099-100).

Such a creating, saving and deleting behavior is extremely unlikely (securely deleting from the camera only the first two photos in one series and all BUT the first two photos in a subsequent series). That the user would just happen to selectively curate and delete photos with consecutive filenames like this – based on content – is not a reasonably credible scenario.

A more plausible explanation is that someone with physical control of the CF Card:

- Recognized the **weak relationship** between the photos reported on the 04/11/2019 CF Card report and those reported as "backup" files on the WD HDD, including alleged contraband,
- Examined the file listing of the WD HDD and chose a convenient range based on **filenames** (IMG_0081-100) rather than their saved **folders**,
- **Created the appearance** (through file and metadata manipulation) that those files had been discovered on the CF Card as reported on the 06/11/2019 report, and
- Botched the file creation and deletion of the new files, rendering them **unviewable** in the 06/11/2019 report.

---

[2] The Modified date/time stamps between the new files in the 06/11/2019 report and their namesakes on the WD HDD did match. However, as explained in my report of Technical Findings, such metadata is easily changed and in this case it was obviously manipulated, enhancing the CF Card – WD HDD relationship required by the Government's narrative.

[3] By *securely deleted* I refer to the process of selectively overwriting physical sectors on the media so that the files cannot be recovered by forensic tools. Selectively eradicating photos in this way is not something a normal user would be able to accomplish. If the deleted photos were recoverable, then the FBI would have included them in the second CF card report.

Conclusion:

The defense team was provided the FBI's forensic report of the CF Card generated on 04/11/2019 and then the second "replacement" report, which was generated on 06/11/2019 and contained 37 additional files.

Along with the appearance of new files on a second CF Card forensic report, it is also undisputed that the **contents of the CF card were modified** on 09/19/2018, while in FBI custody, and that the CF card was delivered to FE Brian Booth in an **unsealed** cellophane bag just two days before FE Booth took the stand.[4] Therefore, in my expert opinion all indications of means, motive, and opportunity point to FBI employees **creating the appearance of additional files** on the CF Card in order to substantiate a relationship between the CF Card and the WD HDD containing the alleged contraband.

[4] These two facts were verified by FE Brian Booth in his sworn testimony.

J. Richard Kiper, PhD, PMP

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

Summary of Process Findings

Professional Background

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

Review of Evidence

My review of evidence includes court testimony, a hard drive copy of logical files, and examination reports generated by members of the FBI's Computer Analysis Response Team (CART). Based on my review, I have observed several technical, administrative, and evidence handling irregularities that raise serious concerns about the integrity of the evidence. Specifically, in this paper I describe violations of processes and procedures which occurred in this case and that likely affected the outcome at trial.

Key Findings

Finding 1: Receiving unsealed evidence created a broken Chain of Custody.

- Neither the camera (Court transcript, p. 4886) nor the CF card (p.4889) was sealed when delivered to CART Forensic Examiner (FE) Brian Booth on 06/10/2019, two days before he took the stand. The FBI Chain of Custody for the CF card (DX 945) indicates that at least three FBI employees – FE Stephen Flatley, SA Elliot McGinnis, and SA Christopher Mills – had physical control of the evidence from the date a reexamination was requested (06/07/2019) to the date it was delivered to FE Booth in an unsealed package (06/10/2019).
- FE Booth's exam notes (DX 961) make no mention of the chain of custody, or of the fact that he received the evidence in unsealed packaging, although in court he admitted it was unsealed when he received it (p.4886 and p.4905). As I will discuss later, FBI policy requires the securing and sealing of evidence, and employees may be disciplined if they fail to do so. In my experience with the FBI, I never received unsealed evidence other than in exigent (emergency) situations.

Finding 2: FBI employees engaged in unusual evidence handling procedures.

- **What normal looks like:** Large FBI offices like the New York Division, where the evidence was processed, have a centralized evidence control and storage facility sometimes referred to as the Evidence Control Unit (ECU). Normally, evidence is collected at a search site by the case agent or a designated seizing agent, and a description of the collected items is entered into Sentinel, the FBI's case management system. Then the agent has up to ten days to physically turn over the evidence to Evidence Control with the chains of custody. After the case agent submits a written request to have the evidence examined, the assigned CART examiner would check out the relevant evidence items from Evidence Control and sign the chains of custody. In her notes (DX 961), Forensic Examiner Trainee (FET) Virginia Donnelly recorded multiple instances where she created derivative evidence items (forensic copies, extractions, and backups of the originals) and turned them into Evidence Control. This is also normal.
- **Abnormalities in this case:** The digital evidence seized on 03/27/2018 seemed to be in and out of the physical control of the case agents, rather than primarily managed through the ECU as described above. Although the evidence was first turned into ECU by the ten-day deadline, it was subsequently checked out by individuals who were not authorized to review digital evidence. The chain of custody for the Camera and CF Card, for example, indicate that the evidence was checked out by SA Maegan Rees on 07/10/2018 for 17 days and by SA Michael Lever 09/19/2018 for seven days – before it was first examined by a CART examiner on 02/22/2019. Both SA Rees and SA Lever indicated "Review" as the reason they were checking the evidence out of the ECU, but **neither of these individuals were authorized to review the contents of unexamined digital evidence**[1].
- Based on my own experience, a case agent would leave digital evidence in the ECU until a CART examiner is requested to check out and examine the evidence. For digital evidence, there is no good reason to check it out of Evidence Control, because the case agent cannot possibly gain any investigative benefit from retaining evidence that he or she cannot examine.
- According to the Chain of Custody for the WD HDD (DX 960), the last person to accept custody of the device was SA Michael Lever, who checked it out from ECU on 02/22/2019. The reason SA Lever provided was "SW," presumably meaning "search warrant," but it is unknown what actions SA Lever took on the WD HDD, or who took custody of the device when he was finished with it. Although the WD HDD had been forensically imaged (copied) by FET Donnelly on 09/19/2018 and processed on 09/24/2018, FE Booth did not generate a report of its contents until 04/11/2019.

[1] In their report regarding the Lawrence Nassar case, the DOJ/OIG made public certain information regarding the FBI's evidence handling procedures: "According to the FBI's Field Evidence Management Policy Guide, evidence must be documented into the FBI Central Recordkeeping System no later than 10 calendar days after receipt. Similarly, the Digital Evidence Policy Guide states that, 'Undocumented, "off the record" searches or reviews of [digital evidence] are not permitted'" (p. 13). (https://oig.justice.gov/sites/default/files/reports/21-093.pdf)

- Finally, FE Booth's examination notes (DX 961) end abruptly after he created a forensic copy of the CF card. Strangely absent from his notes are the options he chose while processing the data with AD Lab, the generation of the "replacement FTK report" presented at trial or the final disposition of the original or derivative evidence. Such details would complete a normal CART forensic report.

Finding 3: The CF Card was accessed by an unauthorized FBI employee.

- According to the FTK reports, the last Accessed dates for active files on the CF card was 09/19/2018 – six months after the CF was collected by investigators and five months before it was first delivered to an authorized CART examiner.
- According to FBI Chain of Custody for the Camera and CF Card (DX 945), the FBI employee who had physical control over the CF card between 09/19/2018 and 09/26/2018 was SA Michael Lever, who recorded "Evidence Review" as his reason for accepting custody (see my Technical Findings report). SA Lever was the primary case agent and not a CART examiner, meaning he was not authorized to review the unexamined digital evidence.
- The FBI's Digital Evidence Policy Guide expressly prohibits any "Undocumented, 'off the record' searches or reviews of digital evidence" and permits investigators to review digital evidence only after it has been processed by an authorized method.[2]
- According to the same Chain of Custody, SA Maegan Rees had previously checked out the Camera and CF card for "Review" on 07/10/2018 and kept them for 17 days. She is also not a CART examiner and also would be prohibited from reviewing unexamined digital evidence. However, if she did access the CF card without a write blocker, then the last Accessed dates would have been overwritten two months later by the actions of SA Lever, who did access the CF card without a write blocker.
- Therefore, there is no doubt the CF card was accessed by at least one unauthorized FBI employee using an unauthorized process.

Finding 4: The CF Card was altered at least once, and likely twice, while in FBI Custody.

- **On 9/19/2018:** File system dates were overwritten on the CF card on at least one occasion, on 09/19/2018, while in FBI custody. This means, at a minimum, that the CF card was accessed without the use of a write blocking device. Failing to preserve digital evidence against alteration is an automatic fail in many of the FBI forensics classes I have taught because write blocking is a critical procedure that, if skipped, becomes an admissibility issue in court.
- **Between 4/11/2019 and 6/11/2019**: According to an FTK forensic report of the CF card completed on 4/11/2019 by "srflatley" (FE Stephen Flatley) and another report completed

[2] *Ibid*, p.13. See also p. 83: "according to the FBI's Removable Electronic Storage Policy Directive, employees may not connect non-FBI removable electronic storage, such as a thumb drive, to FBI equipment without authorization."

on 6/11/2019 by "bsbooth" (FE Brian Booth), several files appeared on the second report that were not included on the first report**.** For reasons I described in my Technical Findings report (see Technical Findings #1 and #2), there is a high likelihood the new files were added to the CF card and altered between these dates. In Appendix D of my Technical Findings report, I explained why adding new files to the CF card could have been used to support the government's narrative regarding the origin of photos on the WD HDD device.[3]

- The difference between the FTK reports cannot be attributed to the use of a different tool, because both examiners used the same tool and version number: AccessData Forensic Toolkit, Version 6.3.1.26.

Finding 5: The FBI Expert Witness knowingly gave false testimony.

- **FE Booth testified that receiving unsealed evidence is not extraordinary (p. 4887).** This characterization by Booth is false, as all CART examiners are trained to receive evidence that has been sealed and initialed.[4] According to FBI evidence handling protocols, anytime a seal is broken on evidence, it must be resealed with a date and initials before relinquishing it to the next person in the chain of custody.[5]
- **FE Booth testified he did not know who had the evidence prior to his examination – two days prior to his testimony.** When he was asked, "And who was it that had access to the camera or the box prior to the time of your examination of it?" FE Booth answered, "I don't have that evidence sheet in front of me to be able to refer" (p. 4889). As mentioned previously, according to FE Booth's examination notes (DX 961), it was the "Case Agent" (but in fact SA Mills) who gave Booth the unsealed camera and CF card on 06/10/2019. It is not credible that FE Booth after two days could have forgotten the person who gave him the one piece of evidence he processed alone during the case.
- **FE Booth repeatedly testified to the reliability of EXIF data,** and that it is "very hard to remove," (p. 4819) and "it's not easily modifiable" (p. 4830). In fact, there are several readily available tools that can easily modify EXIF data. This is a fact that would be well-known to any forensic examiner (see **Appendix A** for a white paper I wrote demonstrating – with screen shots – how easy it is to modify EXIF data). Also, prosecutor Mark Lesko used Booth's false testimony about EXIF data as the basis for his argument that the alleged contraband photos were taken in 2005: "[EXIF] data is

[3] I base this finding on 1) the fact that CF card files were altered, 2) the motive for adding new files (to support the relationship between the CF card and WD HDD), and 3) the opportunity for alteration (the CF card was outside of Evidence Control for several months). This finding could be significantly strengthened (or disputed) if I were to be given access to both forensic copies of the CF card created on 04/11/2019 and 06/11/2019.

[4] The aforementioned DOJ/OIG report (https://oig.justice.gov/sites/default/files/reports/21-093.pdf), p.13 states digital evidence "must be stored and secured and/or sealed to prevent data or evidentiary loss, cross-transfer contamination, or other deleterious change."

[5] *Ibid*, p.83 "Moreover, the FBI Offense Code subjects FBI employees to discipline if they fail to "properly seize, identify, package, inventory, verify, record, document, control, store, secure, or safeguard documents or property under the care, custody, or control of the government."

extremely reliable. It's embedded in the jpeg, in the image itself. And the [EXIF] data shows that the data was created on the camera, in this instance, this particular instance, the 150 jpeg on November 2, 2005 which is consistent with the title of the folder." (p. 5571).

- **FE Booth minimized his knowledge about the previous CF card examination.** On page 4987 of the court transcript FE Booth acknowledged that the government had asked him to create "another report," meaning *in addition to the one created by FE Steven Flatley*. Therefore FE Booth knew, at a minimum, that FE Flatley had conducted an inventory of the camera and CF card, created a forensic copy the CF card, examined it with FTK (AD LAB), and then used FTK to create a report. However, when asked about his knowledge of what FE Flatley had done with the camera and CF card, FE Booth responded, "All I know is that he received it on that date. I have no idea exactly what he's done on the camera" (p. 4988).
- **FE Booth failed to disclose that his actions constituted a prohibited re-examination of digital evidence.** According to FE Booth's notes (DX 961), on 06/07/2019 SA Lever requested that FE Booth "process" item 1B15 (the Camera and the CF card) because FE Flatley "would be overseas during trial."
    - However, according to the Chain of Custody (DX 945) FE Flatley relinquished custody of the CF card to SA McGinnis on this same day (06/07/2019), so he was not yet "overseas."
    - FE Flatley was available to testify to his examination of the CF card, to include the forensic report he generated on 04/11/2019, *at any time during the preceding four weeks of trial*, which began on 05/07/2019. There was no legitimate need to re-examine the CF card and create a second report.
    - If FE Flatley was available to relinquish custody of the physical CF card on 06/07/2019, then he was also available to provide FE Booth with the forensic copy of the CF card he created (and named **NYC024299.001)**. FE Booth should have used the *existing* forensic copy to generate a new report, if needed, rather than creating his own forensic copy.
    - By creating a new forensic copy of the CF card (named **NYC024299_1B15a.E01**), FE conducted a "re-examination" – a duplication of all the technical steps that FE Flatley had already completed. CART policy strictly prohibits such re-examinations, unless approved by the executive management of the FBI Operational Technology Division.[6] I could not find a record of such an approval.

[6] The FBI Digital Evidence Policy Guide, Section 3.3.11.2 states, "Unless approved by the AD, OTD as outlined below, examinations are not conducted on any evidence that has been previously subjected to the same type of technical examination (hereinafter referred to as a 're-examination.')" One of the reasons for this policy is to "[e]nsure that the integrity of the evidence is maintained" (p. 37). A publicly released version of this document, which includes many other requirements for a re-examination, may be found at https://vault.fbi.gov/digital-evidence-policy-guide/digital-evidence-policy-guide-part-01-of-01/view.

    - Instead, according to his notes FE Booth only obtained approval from his acting supervisor Trenton Schmatz to proceed with the re-examination. Given the above facts, therefore, it is not credible that FE Booth had no knowledge of the fact that FE Flatley had already inventoried the camera and CF card, imaged and processed the CF card, and created an FTK report (GX 521A), especially when the government asked FE Booth to create "another report" (GX 521A "replacement"). Also it is not credible that FE Booth did not know his actions violated FBI policy on re-examinations.
- **FE Booth's testimony is especially troubling considering his status as a Senior Forensic Examiner.** In the FBI CART Program, an examiner may apply to be a senior examiner, which requires additional training, additional testing, a research project, and a special moot court exercise. As a Senior Forensic Examiner, Brian Booth should have known his actions were inconsistent with FBI CART policy and his testimony was false and misleading.

Finding 6: The timeline of examination is suspicious.

- 11 months passed between the seizure of the CF card (03/27/2018) and the date it was first delivered to a CART examiner (2/22/2019). As stated previously, several FBI employees – who were not authorized to view unexamined digital evidence – gained physical control of the CF card during that time. FE Flatley was the first CART examiner to receive the CF card and he imaged, then created an FTK report and file listing of the CF card on 04/11/2019. FE Booth first examined the CF card, from which the alleged contraband purportedly came, the day before he took the stand on 6/12/2019 - which was already more than four weeks after the trial began on 5/7/2019.
- It is highly unusual that digital evidence in such a case would be examined for the first time, by the testifying examiner, on the eve of his testimony. In my 20 years of FBI experience I have never seen such a delay – followed by a last-minute examination – in a case with no exigent (emergency) circumstances.

Finding 7: Critical evidence was withheld from the defense team.

- Examination photographs, including those documenting the initial condition of the evidence, were initially withheld (p. 4894). These photographs would include those taken of the evidence by FET Donnelly, FE Flatley, and FE Booth when they received them (on 08/08/2018, 02/22/2019, and 06/10/2019, respectively). In the examination notes of FET Donnelly and FE Booth, the examiners only included photographs of the WD HDD (1B16) and a Lacie HDD (1B28). Conspicuously missing were any photographs of the Camera (1B15) and CF Card (1B15a), as such photographs would document whether or not the evidence packaging was sealed when received by the examiner. Although FE Booth omitted the sealed status of the evidence in his notes, he admitted under oath that

the packaging for neither the camera nor the CF card was sealed when he received them (p. 4886-9).

- When a discovery order is issued by a court, it usually includes documents such as examination notes, reports, file listings, photographs, chains of custody, forensic images, and imaging logs. I have not seen a record of the government providing the CF card forensic image file (or forensic copy) created by FE Flatley (**NYC024299.001**), the CF card forensic image file created by FE Booth (**NYC024299_1B15a.E01**), or any of the logs and .CSV file listings that normally accompany the images. To my knowledge, no one has represented that alleged contraband exists on these forensic images and administrative documents, so there is no reason to withhold them from defense counsel. In **Appendix B** I have listed several of these evidentiary and administrative items that would be crucial to supporting my analysis but were not produced by the government before trial.

Conclusion

Never in my 20 years with the FBI have I seen a case brought to trial with such careless evidence handling, scant documentation, and obvious signs of evidence manipulation (see my Technical Findings report). The points above combined with technical findings of evidence alterations point strongly to the government, at a minimum, being aware that the evidence was unreliable and had been altered.

The government not only withheld this information from the jury but attempted to convey the opposite – that the evidence was reliable and authentic – by eliciting false testimony from FE Booth and making false and misleading statements in their closing arguments.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

Appendix A

A White Paper: EXIF Data and the Case "U.S. vs KEITH RANIERE"

By J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

Introduction

The purpose of this article is to expose the government's mischaracterization of EXIF data used as evidence against the defendant Keith Raniere.

Background

In this case, the prosecution claimed that Raniere used a Canon digital camera to take explicit photographs of a female while she was still a minor, saved them to a compact flash (CF) camera card, transferred them to an unknown computer, and then backed up those photographs to an external hard drive (See Figure 1).

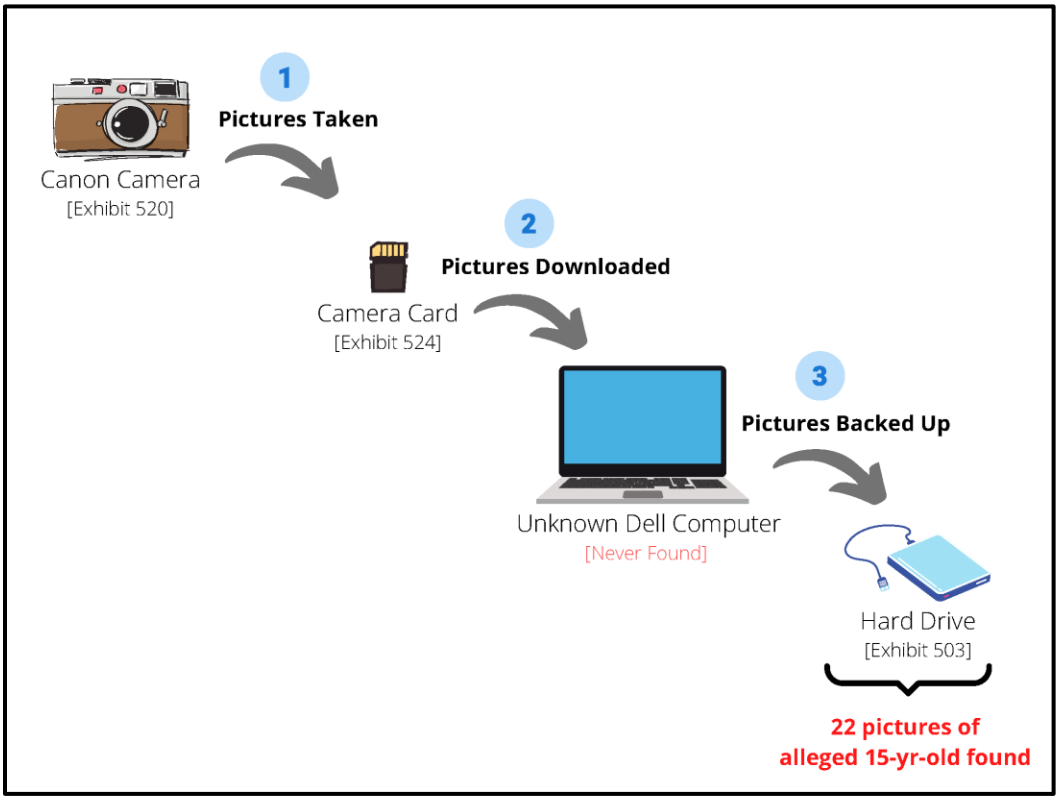


Figure 1: The Government's narrative regarding alleged contraband found on a "backup" drive.

To demonstrate that the alleged user of the camera, Raniere, created the alleged contraband, the prosecution needed to prove two things:

1. The alleged contraband photographs were taken in 2005, and
2. The alleged contraband photographs were taken with the camera allegedly used by Raniere.

The prosecution relied upon information embedded inside the digital photographs, called **Exchangeable Image Format (EXIF) data**, which records how the photo was taken, on what date, and with which camera settings. Since EXIF data is saved into to the *content* portion of the digital photograph file, it does not change when the photograph is transferred to another device.

The prosecution used the photo's EXIF data, specifically their creation date, to argue the subject was underage in the pictures. They also pointed to the fact that the EXIF data of the photos showed the same make and model of the camera allegedly used by Raniere. At first glance, this is a seemingly logical line of argumentation.

But one important question needs to be asked.

How reliable is EXIF data?

According to the FBI's expert witness, Senior Forensic Examiner William Booth, the photo EXIF data – the information that's embedded into the photograph file itself – is extremely reliable because it is "very hard" to change. Consider just a few of his statements from his court testimony (emphasis added):

Question: Is there a particular reason why **EXIF** data is **more difficult** to alter?
Booth: They purposely designed it that way.
Question: Do you know --
Booth: It's mainly to be able to store information. And they don't want data to be moved around and changed, **especially time and date information.** Those things are **very hard for the consumer to be able to modify,** unless you wind up getting **software** that's just developed to do that (p.4820).

Booth: Well, the best reference is the **EXIF** data because that gets put into the JPEG file and it's **not easily modifiable** and it moves with the file the same way from device to device, no matter where you place it. It has nothing to do with the bearing of a file system at all or the dates and times associated with it. So it's on its own, but are created at the same time that you take the picture (p.4830).

Booth: …But when it comes to photos, they still keep you from changing **dates** and **times. It's not easy to change those.** You have to go through **special processes** to change those things. (p.4977)

These are just a few of Booth's statements about the reliability of EXIF data and how hard it is to modify. Prosecutor Mark Lesko emphasized Booth's testimony in his closing argument to the jury:

LESKO: …I'm no expert, don't get me wrong, **but I heard Examiner Booth, just like you did. Exif data is extremely reliable .** It's embedded in the jpeg, in the image itself. And the exif data shows that the data was created on the camera, in this instance, this particular instance, the 150 jpeg on November 2, 2005… (p.5572).

So both the FBI's expert witness and the DOJ prosecutor told the jury they could rely on the photo EXIF data to determine that Raniere had created the alleged contraband with the Canon camera in 2005 because the EXIF data is "extremely reliable" and "very hard" to modify.

However, is it true that digital photograph EXIF data is "very hard" to change? A simple demonstration will help answer this question.

Modifying Photograph EXIF Data

A quick Google search will enable anyone to find many of the freely-available, simple-to-use tools for editing EXIF data. One of my favorites is called **ExifTool**, which was recently featured in an online article titled, "7 Free Tools to Change Photo's Exif Data, Remove Metadata and Hide Dates" (https://www.geckoandfly.com/7987/how-to-change-exif-data-date-and-camera-properties-with-free-editor/). However – as I will demonstrate in a moment – a person doesn't even need to download a free tool to modify EXIF data.

For purposes of the following demonstration, I will use a real digital photograph from the U.S. vs KEITH RANIERE case. Although the photograph with the file name "IMG_0043.JPG" is simply a picture of a tree, it was found on the evidence "backup" hard drive along with the alleged contraband and it was allegedly taken with the same camera at around the same time. In Figure 2 below, the Microsoft Windows details pane (invoked by selecting the "View" tab of any Windows folder) is interpreting some of the EXIF data of IMG_0043.JPG.

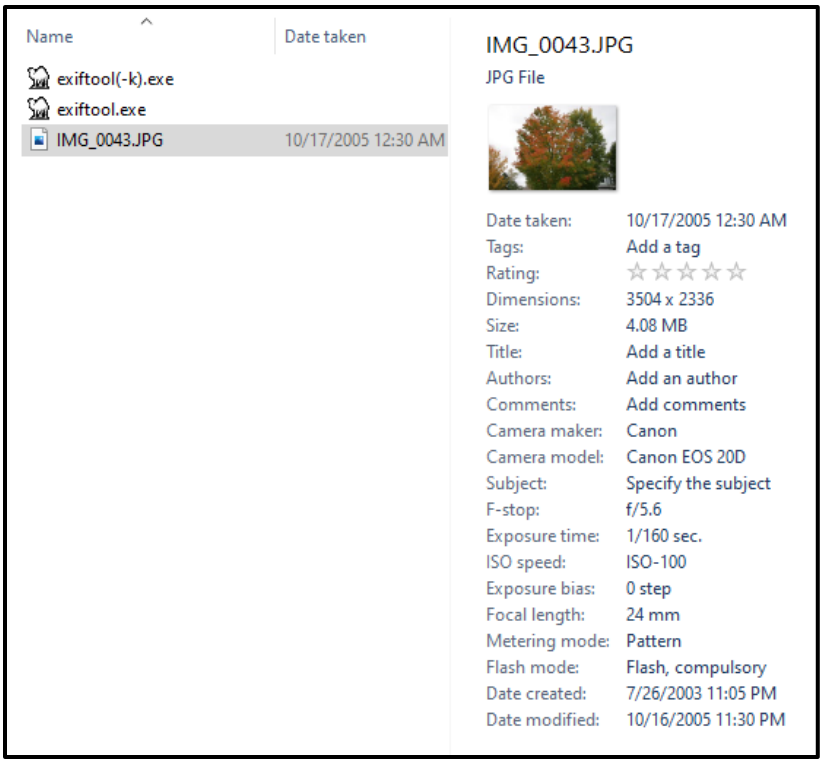


Figure 2. Windows display of EXIF data for IMG_0043.JPG.

According to the Windows display of EXIF data, this photo was taken on **10/17/2005** with a **Canon EOS 20D** digital camera. I verified this information by using the industry standard ExifTool I mentioned earlier. Here is how ExifTool interprets the EXIF data:

```
Make                            : Canon
Camera Model Name               : Canon EOS 20D
Date/Time Original              : 2005:10:17 00:30:04
Create Date                     : 2005:10:17 00:30:04
```

Figure 3. ExifTool display of EXIF data for IMG_0043.JPG.

How hard is it to change the camera model? In the Windows folder with the Details Pane enabled, I simply click the “Camera model” field and type whatever I want. Here I changed the camera model to an iPhone XR.

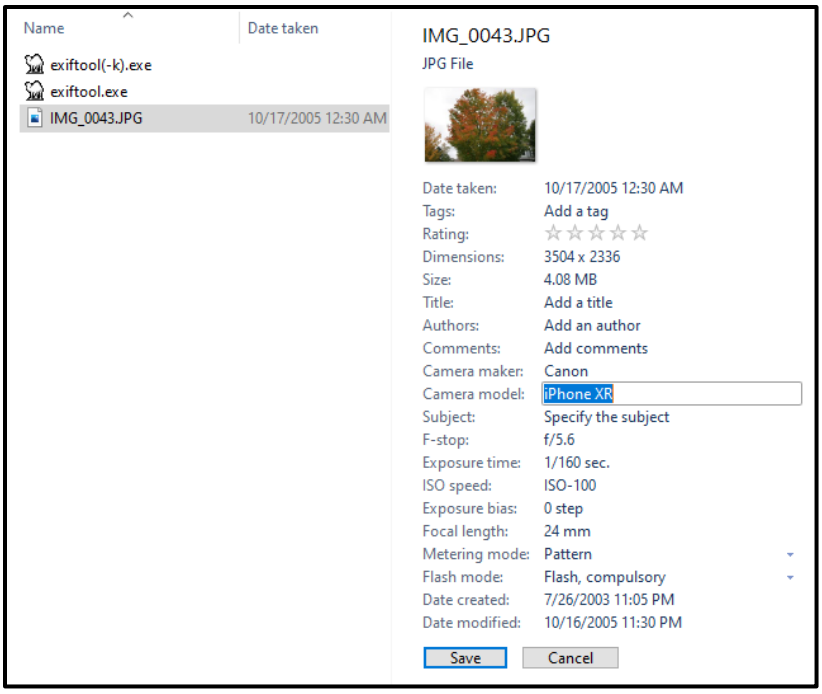


Figure 4. Changing the “Camera model” field in the EXIF data of a photo.

In the same way, I changed the Camera maker to Apple, and then I clicked on the “Date taken” field and set it to the United States Independence Day.

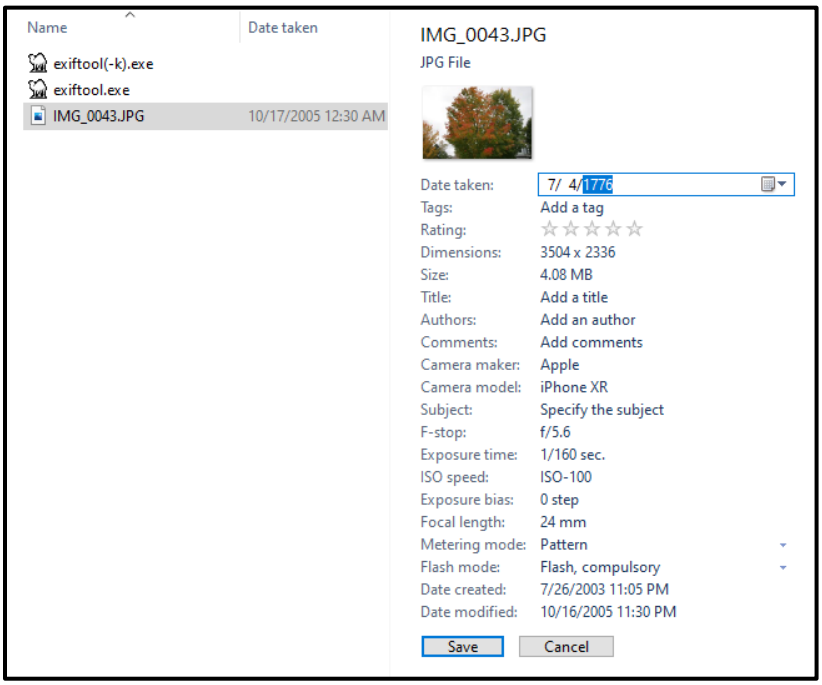


Figure 5. Changing the “Date taken” field in the EXIF data of a photo.

Therefore, a person viewing the file in Windows would now see a photo that was taken by an Apple iPhone XR, in the year 1776.

Figure 6. Windows display of saved changes in the EXIF data of photo IMG_0043.JPG.

Despite the government's contention in court, the EXIF data was very easy to change.

At this point a person might be thinking, "That's fine for the Windows interpretation, but was the EXIF data really modified?" To verify that the changes I made *in the Windows folder* in fact changed the EXIF data *in the file*, I opened the file again in ExifTool:

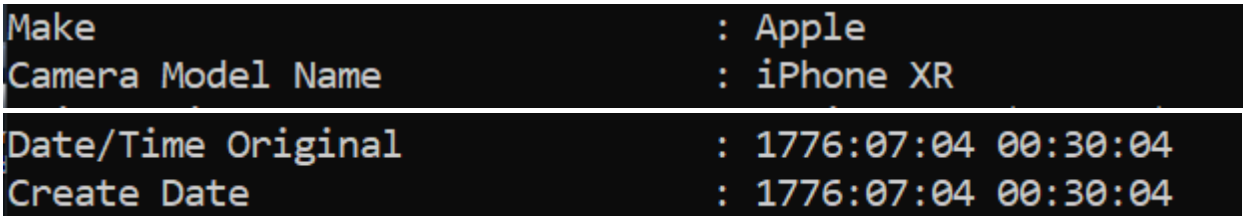


Figure 7. ExifTool display of saved changes in the EXIF data of photo IMG_0043.JPG.

The next question one might ask is: "What about a forensic tool? Would a digital forensic tool verify these changes in the EXIF portion of the file?"

One could argue that ExifTool is indeed a forensic tool, although it is in the public domain. But to put to rest any doubts about what happened, I viewed the photo in one of the most common (and FBI-approved) digital forensic tools available: AccessData's **FTK Imager**. In Figure 8

below, I imported IMG_0043.JPG and used the Hex viewer to read the raw EXIF data. All the EXIF changes I made were readily visible, and there were no traces to indicate that I or anyone else had ever made those changes.

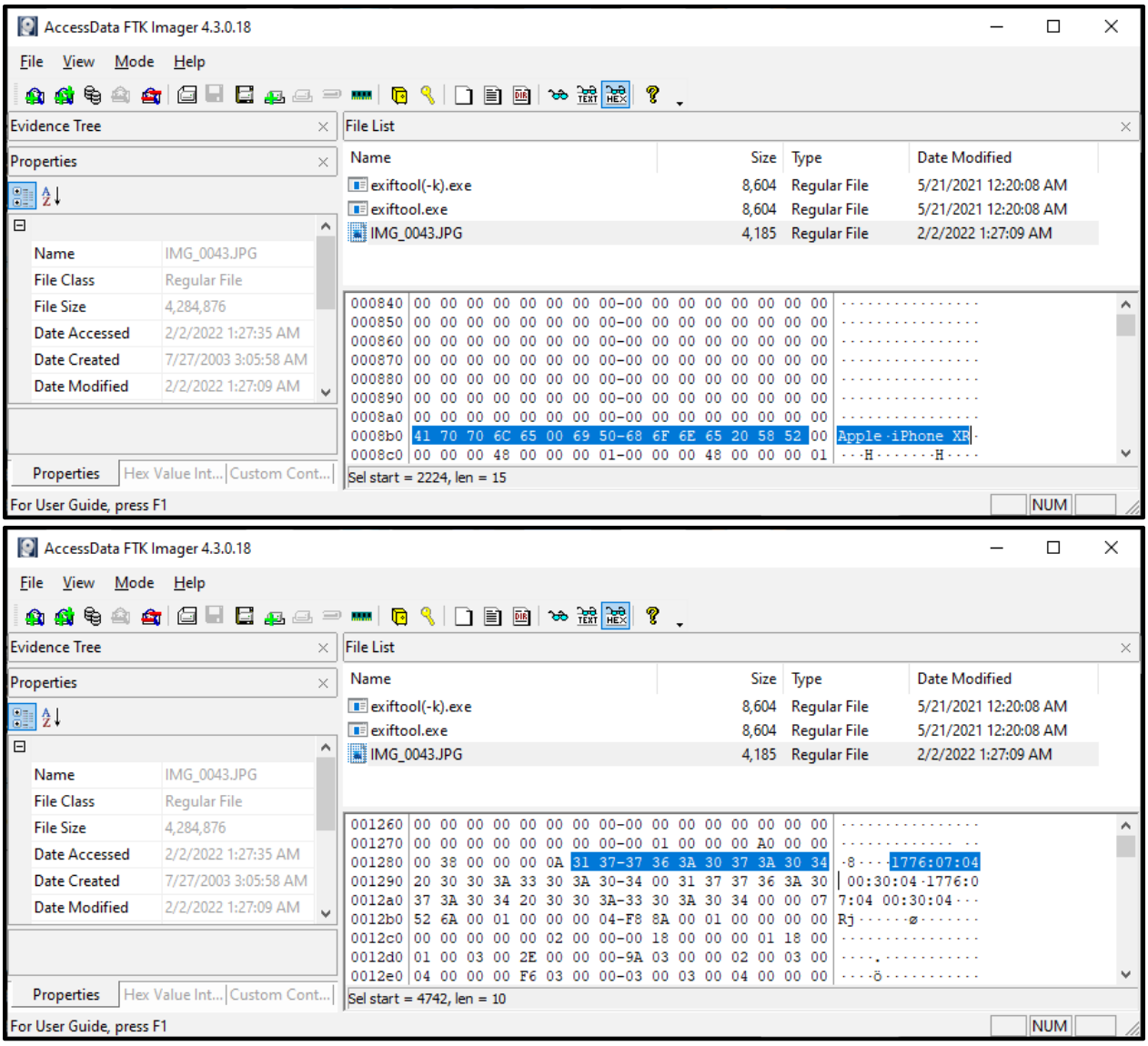


Figure 8. FTK Imager display of saved changes in the EXIF data of photo IMG_0043.JPG.

Conclusion

What does all this mean? It means the government misled the jury about the nature of EXIF data used to convict Keith Raniere.

I could have used one of the many freely available tools to modify the EXIF data that the government claimed was “extremely reliable” and “very hard” to modify. Instead, I simply used the **built-in features of Windows** to modify the EXIF data of one of the actual digital

photographs produced by the government at trial, and then I verified those changes in three different ways. In reality, anyone can reproduce what I just demonstrated in this article, using any digital photograph. Modifying EXIF data requires none of the "software" or "special processes" claimed by FBI examiner Booth, nor is it "very hard" to modify, as he claimed in sworn testimony. It is not clear to me why a Senior Forensic Examiner of his caliber would have made those false statements under oath.

Implications

Why would the FBI's star witness, the digital forensic examiner, swear under oath that EXIF data cannot be easily modified? And why would he make such statements multiple times during his testimony? I just demonstrated how easy it is.

The prosecution needed the jury to believe that EXIF data could not be easily modified because it was the only piece of digital information that supported the narrative that the photos on the drive allegedly belonging to Raniere were of an underage subject. If the prosecution had told the truth – that EXIF data can be easily modified with no special skills or tools – then the jury may have reasonably doubted its reliability as evidence of a crime.

The bottom line: It is a miscarriage of justice for the prosecution (and the jury) to have relied upon the authenticity of EXIF data to prove creation dates and the origin of digital photographs. If the government could blatantly mislead a jury about something so easy to disprove, it leaves me to ponder: What else were they lying about?

Respectfully submitted,

J. Richard Kiper, PhD
FBI Special Agent (Retired) and Forensic Examiner.

Appendix B

Items Requested for Discovery

The following list represents critical evidence and administrative documentation that was not provided to me during my analysis of information pertaining to the case U.S. vs KEITH RANIERE, et al. After serving 20 years as an FBI Special Agent and Digital Forensic Examiner, I know these items should be readily available for the FBI to locate and produce in a timely manner, because most of these items are retrievable from the FBI Sentinel case management system or from the Evidence Control Unit (ECU), which is required to retain evidence for a criminal case until all appeals are exhausted. These items are critical to supporting my analysis of both the digital evidence and FBI procedures in this case, and to my knowledge none of these items were produced by the government before trial.

1. **The forensic image of the CF card (1B15a) created by FE Flatley (NYC024299.001)**, together with its imaging log and file listing (.CSV) file. This is a bit-for-bit duplication of the CF card, and I need to analyze it independently rather than rely on the FBI's submitted forensic reports. If the FBI did not delete it, this forensic image is located on the FBI shared server at: \\nycart-fs\cases05\NY-2233091_208206\Evidence\NYC024299\NYC024299.001. An archive copy should also be stored in the ECU.
2. **The forensic image of the CF card (1B15a) created by FE Booth (NYC024299_1B15a.E01),** together with its imaging log and file listing (.CSV) file. Again, I need to analyze this data independently from the FBI's forensic report, which shows new files were added to the 06/11/2019 report that did not appear on the 04/11/2019 report. My analysis of these two forensic images would determine to a scientific certainty which contents of the CF card were altered while in the custody of the FBI. If the FBI did not delete it, this forensic image is located on the FBI shared server at: \\nycart-fs\CASES02\NY-2233091_196817\Evidence\NYC024299_1B15a\NYC024299_1B15a.E01. An archive copy should also be stored in the ECU.
3. **FE Steven Flatley's complete Examination Notes.** These documents should include the steps taken by FE Flatley during his inventory, imaging, and analysis of the CF card, including software generated log files.
4. **Photographs of the CF card, documenting its condition and packaging, when received by FE Flatley on 02/22/2019 and by FE Booth on 06/10/2019.** FE Booth already testified he received the CF card in an unsealed plastic bag from the case agent. We have no information regarding the condition of the CF card when FE Flatley accepted custody of it.

5. **The original file listing of the WD HDD (1B16) created by FET Donnelly (NYC023721_1B16.E01.csv)** and the imaging log for that item. I need to compare the original file listing to that which was provided to me.
6. **The FTK log (generated by AD LAB) of the processing, browsing, searching, and bookmarking of digital evidence.** I need the FTK logs for the examination of the WD HDD (1B16) and both instances of processing for the CF card (1B15a). Among other important data, the FTK log would capture the date and time SA Lever allegedly "discovered" contraband on the WD HDD.
7. **The CART Requests corresponding to SubID 196817 and SubID 208206**. These documents are normally part of an examiner's "administrative notes," and could help explain the rationale for originally assigning the CF card to FE Flatley while assigning all the digital evidence items (including a reexamination of the CF card) to FE Booth.
8. **All EXIF data for ALL photographs listed on both of the CF card reports** (GX 521A, dated 04/11/2019, and GX 521A Replacement, dated 06/11/2019). I need to compare EXIF data contained in files contained in the forensic images of the CF card with those contained in the WD HDD files. However, if I am provided both forensic images of the CF card (Items 1 and 2) then I do not require this item.
9. **A detailed description (Examination notes) of how GX 504B was generated**, including the tool, options selected, and steps taken. Detailed examination notes are required to be able to replicate the results of the FBI's examinations.
10. **All communications**, including but not limited to texts, e-mail messages, notes, and voicemail messages, of FET Donnelly, FE Booth, FE Flatley, SA Lever, SA Jeffrey, SA Mills, SA Rees, SA McGinnis, AUSA Hajjar, and AUSA Penza, regarding this case. Among the above requested items, this is the only request for information that may not be readily retrieved from the electronic case file or from ECU. However, the communications between these DOJ employees would provide critical context to the actions taken regarding the collection, transportation, storage, and analysis of the digital evidence in this case.

J. Richard Kiper, PhD, PMP

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

Analysis of the Testimony of Special Agent Christopher Mills

Professional Background

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have personally sworn out affidavits for dozens of search warrants and collected, preserved, and analyzed hundreds of pieces of digital evidence. Therefore, I have an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

Introduction

On March 27th, 2018, the FBI executed a federal search warrant at a two-story town home located at 8 Hale Drive, Halfmoon, New York. To my knowledge, the residence had been used as an executive library by Keith Raniere, defendant in the case U.S. vs KEITH RANIERE, et al. As part of my analysis of the digital evidence in this case, as well as the actions taken by the FBI to identify, collect, preserve, and analyze that evidence, I reviewed the testimony of FBI Special Agent Christopher Mills as he answered questions from prosecutor Tanya Hajjar regarding the search.

Among the many curiosities in this testimony, I was particularly struck by the fact that the first two pieces of evidence collected at the residence happened to be the ONLY two pieces of digital evidence used to convict Raniere of child exploitation. It was as if the FBI agents knew what would eventually be “found” on those devices and used at trial.

Moreover, in my opinion the questions by prosecutor Hajjar and the answers by SA Mills seemed specifically choreographed to give the jury the impression that the FBI followed robust procedures during the search, thereby distracting from the subsequent and obvious mishandling of the collected evidence.

Testimonial Analysis

What follows are referenced excerpts from SA Mills' sworn testimony, followed by my analysis regarding their significance to the case.

1. Disproportionate attention to detail regarding search procedures rather than establishing an unbroken chain of custody.

Prosecutor Tanya Hajjar asked, *"Agent Mills, can you just generally describe to the jury what the process is for conducting the search of a residence?" (p. 4290).*

What follows this quote was an unusually long and detailed description of FBI *search procedures*, complete with a discussion of the "knock-and-announce," forced entry, safety sweep, furniture present, search sketch, assignment of letters to each area, movement of agents through the residence, photograph procedures, etc. These 14 pages of detail stand in stark contrast to the vague, one-paragraph description of the *evidence collection and transportation* procedures recorded on page 4307 (discussed in #6, below). For example, the prosecutor introduced the search sketch, the photo log, and all the photos into evidence, but never introduced or even asked about the chains of custody or storage requirements for the evidence that was collected. From a reading of the transcript, it seems the over-emphasis on FBI search procedures was meant to distract from the under-emphasis on evidence handling procedures, which Hajjar must have known was problematic.

2. A new agent, rather than the on-scene case agent, was the sole witness to testify about the execution of the search warrant.

When asked about the search team, Mills answered: *"There was a team, mostly comprised of agents from the New York office, as well as the Albany office" (p. 4291).*

Despite the involvement of a sizeable search team from two different field offices, SA Mills (with only three years on the job) was the *only witness* asked to testify about how the evidence was identified and collected that day. His role was to "assist with evidence collection and documentation" and to take photographs. By contrast, SA Michael Lever, who was the lead FBI investigator in the case (the "case agent"), the affiant on the search warrant, and was probably responsible for the mishandling of the digital evidence for many months after the search[1], did NOT testify during the entire trial. A reasonable person may conclude that the prosecutor intentionally limited the risk of exposing the FBI's evidence mishandling by declining to put the case agent on the stand.

[1] See my Technical Findings and Process Findings reports.

3. The search team ignored several other areas of the residence before starting to search the office.

Hajjir asked, *"And where did you go from there, in terms of initiating the search?" (p. 4294).*

During the unusually long description of the movements of the search team, Mills indicated they moved past the kitchen, living room, bathroom, and open areas of the first floor. Then they took a spiral staircase to the second floor, where they moved through several more areas, including a bathroom, and a seating room area, before finally arriving at the "office space." Although the office was the last of many areas discovered in the residence, it became the first area to be searched. In my experience, the case agent normally assigns groups of FBI personnel to search different areas of the building simultaneously to save time. Working this way in multiple simultaneous locations, search teams would be able to collect evidence, but no one would be able to assign consecutive evidence numbers. In this case, however, someone decided the office would be the first location to start finding AND numbering evidence.

4. The very first item to be identified in the entire residence was a camera with a camera card, located under a desk, and which happened to be one of two key pieces of digital evidence used to convict Raniere of child exploitation.

In describing one of the search photographs he took, SA Mills said, *"So the there's a note there with the number one. So number one represents evidence item number one. So, in this case, this photo was taken underneath the desk or table and was assigned number one based on being the first evidence item that was found" (p. 4304).*

If SA Mills' account is correct, then the FBI search team traversed several areas of the residence, went upstairs and straight to the office area, and then crawled under a desk to find the first piece of evidence – a camera bag containing a camera and camera card. At this point, the case agent, SA Lever, had not yet "discovered" alleged child pornography taken with this camera, so it seems more than a strange coincidence that it was the first evidence item identified.

Another anomaly is the fact that an item number was assigned to the camera immediately upon discovery. All the items documented in the photo log (GX 502) and represented in the photographs (GX 502A) have item numbers, written on sticky notes photographed next to the items. Generally, FBI search personnel do not assign item numbers to evidence at the moment of discovery/photography/collection, because there are multiple people working in different rooms and it would be impossible to coordinate the numbering among them. If any items are assigned item numbers, then it is done near the *end* of the search when the seizing agent collects all the evidence together and fills out the FD-597 receipt for items seized. Therefore, in practice the item numbers rarely correspond to the order in which they were collected.

5. The very next item to be identified in the entire residence was an external hard drive, located away from the desk on a shelf, and which happened to be the second of two key pieces of digital evidence used to convict Raniere of child exploitation.

When asked about another photograph he took, SA Mills answered, *"So this is the still of the same office space as seen before and item number two, which is on top of the bookshelf here, is a gray or silver hard drive" (p. 4308).*

Once again, it is extremely convenient that from all the potential evidence in the residence, it was the Western Digital hard drive – where the alleged child pornography was stored – that was the *second* piece of evidence identified by the FBI on scene. It is also important to note that the camera card (Item #1) and the hard drive (Item #2), comprised the entirety of the child exploitation digital evidence against Raniere – which supposedly was not "discovered" by the FBI for nearly a year later.

6. Prosecutor Hajjar did not even attempt to establish an unbroken chain of custody for the digital evidence used against Raniere.

Hajjar: *What happens when you recover a piece of digital evidence like Government Exhibit 520 and 524?*

Mills: *So, when we receive -- when we recover digital evidence, we have a process in which we bring the digital evidence back to our office and if we want the evidence to be reviewed, we would submit a request to our CART team. And the CART is the Computer Analysis Response Team and they have specialists who are computer evidence examiners who would review that evidence for us or assisted us in reviewing the evidence with us.*

Hajjar: *And is that what happened in this case with Government Exhibit 520?*

Mills: *Yes.* (p. 4307).

After spending several minutes eliciting the details of search activities, the prosecutor was strangely disinterested in establishing an unbroken chain of custody for the two pieces of digital evidence presented at trial. Conspicuously missing were the following questions, for example:

- Who decided which pieces of evidence were relevant and within the scope of the search warrant?
- Why did you bypass documents and other potential evidence in other rooms in order to start with items in the office?

- While in the office, why did you start identifying and collecting evidence beneath the desk?
- The photo log shows that you went back and forth from room to room, photographing various evidence items there. Why didn't you stay in one room to photograph all the evidence there, before moving on to the next room?
- Who decided the order in which the items were to be photographed and assigned item numbers?
- After you photographed each piece of evidence, what specifically did you do with it?
- Who sealed the evidence?
- Who packaged the evidence?
- Who started the chains of custody for the evidence?
- Who transported the evidence back to your office?
- Who took custody of the evidence at the office, and how was it stored?
- You said you found the camera card (CF card) inside the camera (p. 4305). You must have removed it on scene to identify it here in court. Who removed it permanently and put it inside a cellophane bag?
- Why didn't you photograph the CF card after you discovered it inside the camera?
- Why wasn't the CF card noted on the photo log, chain of custody, electronic evidence entry, or any other documentation related to the seizure of the camera?
- When was this evidence relinquished to case agent Michael Lever?
- How long did he have custody of the evidence?
- Did you realize that the camera and the CF card were in unsealed containers when you regained custody and relinquished them to FE Booth on 06/10/2019?
- Who unsealed them and why were they not re-sealed?

In the above trial excerpt, it seems the prosecutor specifically crafted her sentence to avoid discussing *who* in the FBI had taken actions on the digital evidence after it was identified at the search site. As I detail in my Process Findings report, the chains of custody demonstrate that SA Lever and other FBI individuals not authorized to review unexamined digital evidence gained physical control over the digital evidence for several months before turning it over to CART forensic examiners. In fact, the CF card was checked in and out of the Evidence Control Unit (ECU) for eleven months before it was finally released to the first CART examiner, Stephen Flatley, on 02/22/2019. During that time, as the government has acknowledged, an FBI employee accessed that camera card on 09/19/2018. The Chain of Custody indicates that the case agent, SA Michael Lever, had custody of the CF card from 09/19/2018 to 09/26/2018. In my Technical Findings report, I describe several anomalies that demonstrate manual manipulation of data on that card.

The Chain of Custody also shows that other FBI employees, SA Elliot McGinnis and SA Christopher Mills, regained custody of the camera and CF card from the first CART examiner

before turning it over to a second CART examiner, Brian Booth, in *unsealed packaging* on 06/10/2019 – *the very day Mills testified about collecting it*. As explained in my Process Findings report, a second examination of digital evidence is strictly prohibited by policy, and for the second examiner to receive the original evidence from a case agent (rather than using the work of the previous examiner) is very abnormal.

Regarding SA Lever's handling of the digital evidence in this case, there are several questions that must be answered, for example:

- Why did SA Lever and other FBI employees check out the evidence from the ECU multiple times, when they were not authorized to even look at it?
- Why did SA Lever access the CF card without a write blocker on 09/19/2018?
- Why does the Chain of Custody for the WD HDD (DX 960) end with SA Lever checking it out of Evidence Control on 02/22/2019?
- What did SA Lever do with the WD HDD after he checked it out?

It is very telling that the prosecutor completely avoided the topic of chain of custody with respect to the digital evidence in this case.

7. Sometime after collecting the first and only two pieces of digital evidence eventually used at trial, the searching agents returned to the space beneath the desk and collected another external hard drive.

After being asked to describe another photograph he took, SA Mills said, *"So this is, once again, underneath the desk or the table in the office space. And you see item number 14, so that's evidence item number 14, the gray or silver hard drive" (p. 4310).*

SA Mills later identified this second external hard drive as a LaCie external hard drive (Item #14). If (according to SA Mills) the item numbers correspond to the order in which they were collected, then this item was *discovered in the same place as the camera bag* (Item #1) – yet it was not discovered and collected until much later. In fact, according to the seized property receipt[2] and the search photos (GX 502A), the FBI collected a book, 30 cassettes, an Amazon Kindle, two CD discs, a thumb drive, and miscellaneous documents before returning to the space beneath the office desk to collect the LaCie hard drive and other computer equipment.

This strange behavior begs the following question: Why did the FBI agents first go straight to the camera bag (Item #1), located under the desk, then search a shelf, where they retrieved an external hard drive (Item #2), then collect dozens of other items (some found in other rooms) before returning under the desk, where they found the LaCie external hard drive?

[2] See FD-597, Receipt for Property Seized.

Conclusion

The prioritized collection of the only two pieces of digital evidence used to support the child exploitation charges at trial (Items #1 and #2) strongly points to foreknowledge on the part of the FBI agents. In fact, a reasonable person would suspect the evidence collection process itself was influenced by someone with an interest in the FBI "finding" digital evidence against Raniere.

Moreover, the question-and-answer interactions between prosecutor Hajjar and SA Mills seemed intent on convincing the jury of the reliability of the digital evidence through a robust discussion of FBI *search* procedures, while deliberately obfuscating the FBI's *aberrant evidence handling* activities that occurred thereafter. In short, the testimonial evidence recorded in this court transcript is consistent with the evidence manipulation opinions and conclusions expressed in my Technical Findings and Process Findings reports.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

J. Richard Kiper, PhD, PMP

FBI Special Agent (Retired) and Forensic Examiner

April 25, 2022

Expert Opinion Regarding Time to Review Digital Evidence

Professional Background

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics (See attached CV). In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have personally sworn out affidavits for dozens of search warrants and collected, preserved, and analyzed hundreds of pieces of digital evidence. Therefore, I have an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

Review of Events

In my experience serving in the FBI's Computer Analysis Response Team (CART), forensic examiners are typically given several months to examine digital evidence and prepare analyses for legal proceedings. Similarly, a court's discovery order usually requires that evidence against the accused be provided to the defense team with enough time to prepare a reasonable defense. In the case of U.S. vs KEITH RANIERE, neither of these norms were followed.

Two digital devices – a camera card (CF card) and an external hard drive (WD HDD) – were the only pieces of digital evidence used to support the government's charge of child exploitation in this case. However, despite having possession of these items for a year, the FBI did not provide defense counsel any access until 03/13/2019[1], a mere twenty-six days before jury selection was scheduled. At that time, the FBI gave the defense access to the forensic image of the *external hard drive only*, and due to the allegation of child pornography, the defense expert could not remove any data from the premises beyond screen shots of file listings and handwritten notes.

Further impeding the ability of the defense to conduct a thorough review of the evidence with its own forensic tools, the FBI did not provide a "clean" (non-forensic) copy of the contents of the hard drive until 04/06/2019, less than a week prior to the scheduled jury selection.

[1] This was also the date of the government's Second Superseding Indictment alleging sexual exploitation of a child. According to the FBI examiner's notes, 03/13/2019 was the date the hard drive image was prepared for review. I do not know when the defense expert was provided access to review it.

Finally, the FBI significantly delayed the creation and delivery of the forensic reports used at trial. According to the sworn declaration of defense counsel Marc Agnifilo filed on 04/22/2019, "…when asked recently when we were going to get these reports, the prosecution stated that the reports were not completed but that the government would make the reports available when the FBI completed them." In fact, the "not completed" forensic reports already had been completed on 04/11/2011 but *were still being withheld from the defense team two weeks prior to opening statements*.

The government's delay of the second forensic report of the CF card was even more egregious. The FBI first examined the CF card and created a forensic report on 04/11/2019. Then, more than four weeks AFTER trial had begun – and against FBI digital evidence policy – the FBI conducted a *second examination* of the CF card[2] resulting in a *second forensic image* and generated a "replacement" report of the CF card on 06/11/2019. The defense team literally had no time to prepare a technical rebuttal before this report was introduced at trial.

Required Analysis

A defendant is entitled to the opportunity to review, analyze, and rebut the evidence used against him. At a minimum, the analysis of digital evidence in this case should have included the following tasks:

- A review of the legal authority to conduct the examination.
- A review of the evidence collection, packaging, transportation, and storage procedures.
- A review of the chain(s) of custody.
- A review of the examination notes and administrative paperwork.
- Verification of evidence integrity (e.g., via MD5 hashing).
- Reproduction of the forensic steps used to produce the alleged results.
- New analysis of evidence, including but not limited to:
    - File system metadata,
    - EXIF data,
    - File content,
    - Application artifacts,
    - Operating system artifacts, and
    - Timeline analysis
- Creation of new trial exhibits to rebut the government's narrative.

In my expert opinion, it would be impossible for a defense expert to have completed the above listed activities within a mere twenty-six days (in the case of the hard drive) much less instantaneously (in the case of the CF card).

[2] See my Technical Findings and Process Findings reports, where I describe this anomaly in detail.

Conclusion

The government placed the Raniere defense team at a significant and unjust disadvantage by intentionally withholding key evidence they intended to use at trial. At best, the defense team was given only twenty-six days to conduct a technical review of *some* of the digital evidence (a non-forensic and partial copy of the hard drive contents) and at worst, it was given *no opportunity* to review the second FTK forensic report related to the CF card.

It is my expert opinion that it was unreasonable to expect the defense team to have conducted a forensic analysis of the digital evidence in this case within the given time frames.

Respectfully Submitted,

J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

Appendix B

Affidavit of Dr. James Richard Kiper, Ph.D.

State of Florida
County of Leon

COMES NOW Dr. James Richard Kiper, Ph.D., being first duly sworn, under oath, and states that the contents of the following attached report(s), including their appendices, and exhibits are true and correct statements of relevant facts and his opinions in the case of United States v. Keith Raniere et. al., in the United States District Court, Eastern District of New York, Case #: 1:180-cr-00204-NGG-VMS, to the best of his knowledge and belief:

- Flatley versus Booth: An Analysis of Conflicting FBI Testimony Regarding EXIF Data

Signature: _____

Address: 818 Shannon Street
Tallahassee, Florida 32305

SUBSCRIBED AND SWORN TO before me this 6th day of Sept., 2022, by James R. Kiper.

Physically appeared and attested before me.

_____
NOTARY PUBLIC FOR FLORIDA

DOUGLAS E WRIGHT
Commission # GG 293252
Expires March 22, 2023
Bonded Thru Budget Notary Services

My Commission Expires: 3-22-23

J. Richard Kiper, PhD, PMP

FBI Special Agent (Retired) and Forensic Examiner

September 5, 2022

Flatley versus Booth:
An Analysis of Conflicting FBI Testimony Regarding EXIF Data

Professional Background

I served as an FBI Special Agent for 20 years, from 1999 to 2019, with more than half of that career in cybersecurity and digital forensics. In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have personally sworn out affidavits for dozens of search warrants and collected, preserved, and analyzed hundreds of pieces of digital evidence. Therefore, I have an in-depth knowledge of FBI evidence handling procedures, and of digital evidence examination procedures and policies.

Introduction

In the case U.S. vs KEITH RANIERE, et al. the government contended that Raniere used a digital camera to take explicit photographs of women, saved them to a camera card, transferred them to an unidentified computer, and then backed them up to an external hard drive. The camera card and the "backup" hard drive comprised the only digital evidence used at trial. According to the government's narrative, all the backed-up photographs were taken in the year 2005, at a time when one of the women was 15 years old. **The government argued if the pictures were taken in 2005, then 22 photos of the backed-up photos would constitute child pornography.**

In order to date these photographs, the government relied on two pieces of digital information – the names of the folders containing the photos and the "Create Date," saved inside the content portion of the photo called EXIF data. The problem is that both pieces of data are forensically unreliable. Any computer user who has created a folder realizes how easy it is to modify a folder name. And while fewer people know how to modify the embedded "Create Date" in a photo's EXIF data, I have conclusively demonstrated the ease of modifying this data using Windows functionality with no special skills or tools.[1] Nevertheless, the government insisted that EXIF data is "hard to change" and "is extremely reliable."[2]

---

[1] See my Summary of Process Findings report, Appendix A for a full demonstration and debunking the government's claim that EXIF data is "very hard to modify," found at *United States v. Raniere*, 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D.

[2] *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Trial Transcript hereafter, "Trial Tr.," at p.4977; 5572.

Senior Forensic Examiner (SFE) Brian Booth was the FBI's expert witness who testified under oath as to the reliability of EXIF data. He did so after being requested to conduct a *second forensic examination* of the camera card, which he had received in an unsealed package during the final days of the trial.[3] SFE Booth produced a "replacement" forensic report of the camera card on 06/11/2019, and it contained 37 additional files *not included in the first FBI forensic report*. Although 31 of the 37 new files had namesake counterparts on the alleged backup hard drive, the new files had several issues with *metadata* and showed dispositive evidence of manual alterations.[4]

SFE Stephen Flatley[5] was the first forensic examiner to examine that camera card and had produced a report two months earlier, on 04/11/2019. However, the government declined to put SFE Flatley on the stand to explain his report. Instead, during the fifth and final week of trial the government abruptly gave SFE Flatley an overseas assignment and through the hands of several people transferred the camera card to SFE Booth in an unsealed package.

Until recently, the government's refusal to use SFE Flatley and his report during the first four weeks of trial was an inexplicable decision. However, I believe SFE Flatley's testimony on a *previous case* could shed some light on this mystery. As I will explain in the following pages, SFE Flatley's previous testimony *directly contradicted* SFE Booth's testimony regarding the reliability of metadata dates, and to be consistent SFE Flatley *likely would not have supported the government's claims* in U.S. vs KEITH RANIERE.

The 2016 Trial Testimony of SFE Stephen Flatley

On 09/20/2016, SFE Flatley was called to testify as the government's expert witness in the case U.S. vs GARY HIRST.[6] After qualifying SFE Flatley as an expert witness, prosecutor Brian Blais immediately began questioning SFE Flatley on the topic of *metadata* and *dates*:

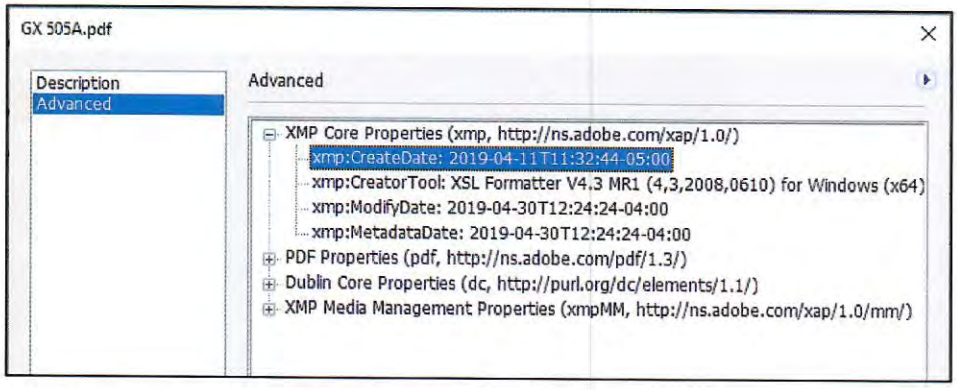
Q. Where is **metadata stored**?
A. There is two different places overall where it could be stored. It could be stored in the computer's file system in the computer itself. So the overall **creation date** of the file could be stored there. Certain files also have **metadata stored inside them.** Things like Word documents, **PDF documents,** some photographs, like **JPEGs** and a certain type called **JPEG Exif** will have certain other aspects of metadata inside of it.
Q. How is metadata generated?
A. It's generated at the time the file is created, and **then it can be modified** at later dates.[7]

---

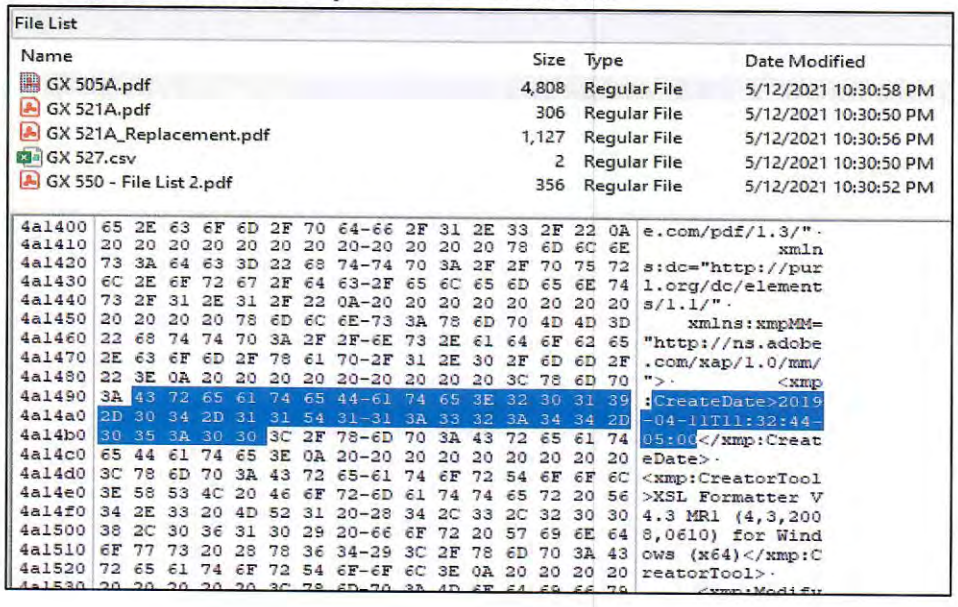
[3] See my Summary of Process Findings report for further details, found at *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D.
[4] See my Summary of Technical Findings, Finding's #1 and #2, found at *Id.*
[5] For full disclosure, I am acquainted with SFE Flatley personally and have co-instructed with him while serving as a digital forensics instructor in the FBI.
[6] *United States v. Hirst*, 15-cr-643 (PKC) (SDNY Apr. 18, 2022).
[7] *Id.* at Trial Transcript hereafter, "Trial Tr.," at p. 935:24-936:9.

During this exchange, it was appropriate for SFE Flatley to mention the similarity of metadata stored inside PDF documents with that stored inside JPEG (photo) files as EXIF data. Indeed, PDF files and JPEG files store "Create date" information in essentially the same way – by inserting the date and time into the content of the file.

To illustrate this fact, I opened the PDF document Government's Exhibit "GX 505A.pdf," representing the FBI's forensic report of the external hard drive in this case. By clicking File > Properties > Additional Metadata I could view the imbedded "Create Date" of the document as 04/11/2019.

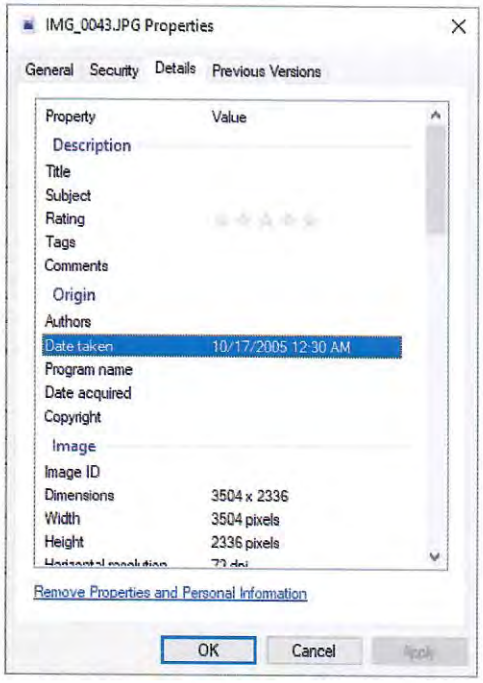


Using a forensic tool, FTK Imager, I verified that the date is indeed part of the *content* of the file, rather than stored elsewhere in the file system, by opening the same GX 505A.pdf document and viewing the hexadecimal representation of the data:



Using these two screen shots, one can observe the imbedded date/time of "04/11/2019 11:32:44" is saved as the "Create Date" value inside the content of the "GX 505A.pdf" file. This is exactly what SFE Flatley was describing during his testimony.

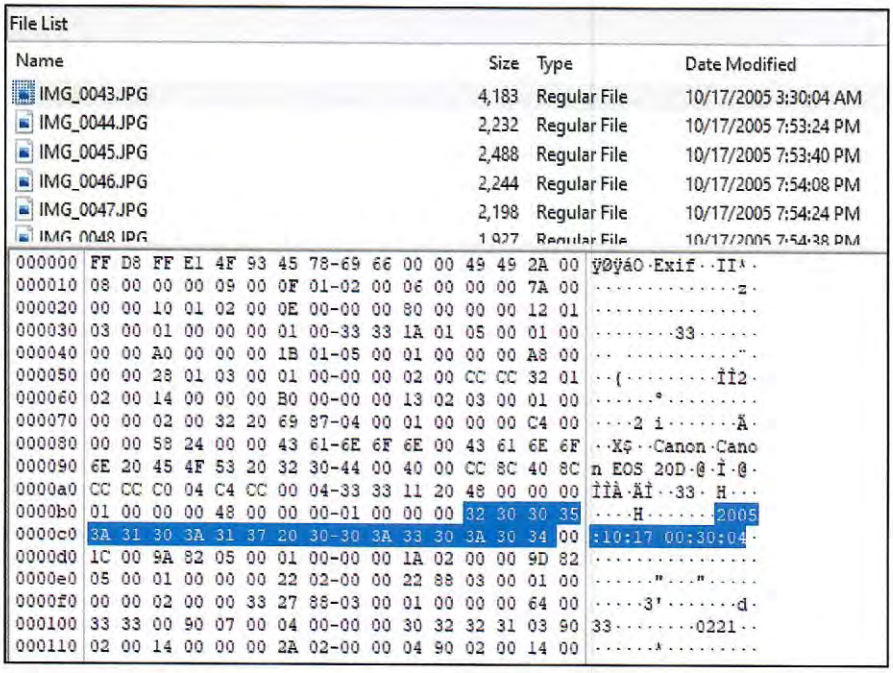
As SFE Flatley mentioned during his testimony, JPEG photo files also contains metadata, stored essentially in the same way, inside the content of the file as EXIF data. In the following screen shot I viewed the properties of "IMG_0043.JPG," a JPEG photo file in this case. The EXIF create date is displayed as "10/17/2005 12:30AM" which is interpreted by Windows as "Date taken."



Loading this file into another program, Exiftool, one observes the name of metadata create date of the JPEG is identical to that of the PDF, which is "Create Date":

```
C:\Photos>exiftool ./Originals/IMG_0043.JPG |find "Date"
File Modification Date/Time     : 2005:10:16 23:30:04-04:00
File Access Date/Time           : 2022:09:01 14:09:31-04:00
File Creation Date/Time         : 2022:02:28 13:48:56-05:00
Modify Date                     : 2005:10:17 00:30:04
Date/Time Original              : 2005:10:17 00:30:04
Create Date                     : 2005:10:17 00:30:04
```

Using the same procedure used for the PDF document, I opened the JPEG file using FTK Imager and verified the date in the *content* of the photo file:



Although the majority of SFE Flatley's testimony addressed metadata embedded inside PDF documents, he immediately drew a similarity to metadata inside of JPEG photo files. Indeed, as the above exercise demonstrates, they are essentially created and stored in the same way.

More importantly, SFE Flatley stated *another aspect* of metadata in the transcript excerpt cited above. Immediately after mentioning JPEG EXIF data, SFE Flatley revealed that metadata stored inside of files "**can be modified at later dates**." How? SFE Flatley testified that Exiftool and Xpdf, two freely available software tools, may be used to modify metadata in JPEG and PDF files. In fact, with respect to these publicly available metadata authoring tools, SFE Flatley testified, "[T]here's a bunch of them."[8] How would a person obtain such a tool? SFE Flatley testified, "You just download it from the web."[9]

The Unreliability of Embedded Metadata Dates

Because their determination of *child pornography* solely depended on the *created dates of the photographs*, the FBI's expert witness SFE Booth and DOJ's prosecutor Tanya Hajjar went to great lengths to convince the jury of the reliability of EXIF data. What follows are just a few statements from their exchanges during trial (emphasis added):

Q. Is there a particular reason why **EXIF** data is **more difficult** to alter?
A. They purposely designed it that way.
Q. Do you know --

[8] *Hirst, supra,* 15-cr-643 (PKC) Trial Tr. at p.936:17-21.
[9] *Id.* at p.941:22-942:3.

A. It's mainly to be able to store information. And they don't want data to be moved around and changed, **especially time and date information.** Those things are **very hard for the consumer to be able to modify,** unless you wind up getting **software** that's just developed to do that[10]

Later in his testimony, SFE Booth admitted that the *file system* Created date for all the "backed up" photos, including the alleged contraband, was in 2003. This would mean the photos were copied to the external hard drive *two years before* the government claimed they were taken – a physical impossibility. Therefore, after recognizing they could not rely on the *file system* create dates for the backup files[11], SFE Booth and prosecutor Hajjar turned their attention back to the easily-modifiable *EXIF data* to support the create date they needed the jury to believe.

Q. You testified that the EXIF data shows the date and time associated with this is October 18, 2005?
A. Yes.
Q. And so between the dates here and the EXIF data, what's the **best evidence** of when this photograph was taken?
A. Well, the best reference is the **EXIF** data because that gets put into the JPEG file and it's **not easily modifiable** and it moves with the file the same way from device to device, no matter where you place it. It has nothing to do with the bearing of a file system at all or the dates and times associated with it. So it's on its own, but are created at the same time that you take the picture[12]

These are just a few of SFE Booth's statements regarding the reliability of EXIF data and how difficult it is to modify. The court transcript records *15 pages* of SFE Booth and prosecutor Hajjar mischaracterizing the reliably of EXIF metadata[13]. Again, to support their narrative that the alleged contraband photos were taken in 2005, the government needed the jury to believe the reliability of the metadata.

The reliability of the EXIF data was so crucial to the government's charge of child pornography, prosecutor Mark Lesko emphasized Booth's testimony during his closing argument to the jury:

LESKO: ...I'm no expert, don't get me wrong, **but I heard Examiner Booth, just like you did. Exif data is extremely reliable.** It's

---

[10] *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Trial Transcript hereafter, "Trial Tr." at p. 4820:2-20.
[11] *Id. at* Trial Tr. at p. 4829:12-24 [emphasis added], From Booth's trial testimony: ["As you move things from one computer to another, if the times are different and they're different types of file systems, they'll get a new created time and if dates are wrong, they can be ***manipulated***...Usually, if anything, it would be the created time that would be changed. Sometimes you can get a created dated that's after your modified date, which happens when you just happen to move to a different type of file system later on after you've had the file. But in this case, it's actually **reversed.** *Somehow it got changed to where the date is well, well, before then what might be the first modified date or a modified date.*"] On cross examination, SFE Booth openly admitted that the file creation dates for all the "backed up" photos, including the alleged contraband, were unreliable: "...The file system metadata for those dates and times are not accurate" *Id.* at Trial Tr. at p. 4941:1-19. Hence, to support the 2005 create date the government needed the jury to believe in the reliability of JPEG EXIF data.
[12] *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Trial Tr. at p. 4829:25-4830:11.
[13] *Id.* at Trial Tr. at p. 4816-4831.

embedded in the jpeg, in the image itself. And the exif data shows that the data was created on the camera, in this instance, this particular instance, the 150 jpeg on November 2, 2005….[14]

SFE Flatley, the FBI's expert witness in a previous trial, would disagree:

Q. Now, Mr. Flatley, does the FBI **rely** on **creation dates alone** in PDF files in determining the date on which that PDF file was, in fact, created?
A. **No, we do not do that.**[15]

Earlier in this paper, I demonstrated that PDF files and JPEG files use the same method for storing metadata for creation dates. In fact, PDF files and JPEG files even use the *same metadata tag*, "Create Date" to record this information. Since SFE Flatley discussed the composition of JPEG files alongside PDF files in his testimony, he would similarly testify that the FBI does NOT rely on creation dates alone in determining the date on which a JPEG file was created.

Why not? According to SFE Flatley, the FBI "would require that we have some kind of corroborating evidence."[16] To rely upon the metadata "Create Date" in either a PDF or JPEG file, the FBI would require corroborating data from other devices and mechanisms that possibly stored or transmitted the file, but these devices must be "outside the user's control."

A. So something that was not just from the standalone system that would require some kind of corroboration or something outside the user's control.[17]

Despite SFE Flatley's claim to the contrary, in the case U.S. vs KEITH RANIERE, the FBI used no other devices, systems, or mechanisms to corroborate the easily-modifiable EXIF metadata dates in the JPEG files. Instead, the FBI consistently claimed EXIF metadata was reliable by itself and difficult to change, as SFE Booth testified on cross examination:

A. …But when it comes to photos, they still keep you from changing **dates** and **times. It's not easy to change those.** You have to go through **special processes** to change those things.[18]

By contrast, SFE Flatley gave a very different answer when asked for reasons why a create date "reflected in the file's metadata may not match the actual creation date." SFE Flatley testified to several reasons why file metadata dates are unreliable:

---

[14] *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Trial Tr. at p. 5572.
[15] *Hirst, supra,* 15-cr-643 (PKC) Trial Tr. at p.939:15-18.
[16] *Id. at* Trial Tr. at p.940:9-23.
[17] *Id.*
[18] *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Trial Tr. at 4977:11-14.

A. A computer's clock is too easily changed. It's very easy to go down and change your time and date on the machine. It's also a standalone system. It could just flat be wrong. The clock could be off, it could have been changed either inadvertently or by, what's the word I'm thinking of, just, you know, just out of habit or something of that nature that they just change the time, date. Also, your machine, when it's off, relies on a battery to keep the clock up. It's called the cmos battery. If that battery dies, the clock will revert to its beginning.[19]

Just as SFE Booth repeatedly testified that the FBI considered metadata create dates ***reliable***, SFE Flatley repeatedly testified that the FBI considered metadata create dates ***unreliable***:

Q. Based on your training and experience, would the FBI **rely** on the **create dates alone** in the metadata of Government's Exhibits 509A through D in determining the dates on which these documents were created?
A. **No, we would not.**[20]

SFE Flatley's position regarding the unreliability of metadata create dates was not an ancillary opinion – it was the entire purpose for his testimony. As the prosecutor concluded his direct examination:

Q. So Mr. Flatley, in your opinion, can you conclude that Government's Exhibits 509A through D were **created on the dates** reflected in the **metadata** in those documents?
A. **I cannot.**[21]

Conclusion

In the case U.S. vs KEITH RANIERE it is notable that SFE Flatley, an FBI expert witness who previously testified to the unreliability of metadata create dates, was *replaced* in the last week of trial by SFE Booth, who testified to the reliability of metadata create dates. And although the government did not allow SFE Flatley to testify in the RANIERE case, much of his prior testimony directly supports the findings in my Summary of Technical Findings report.[22]

---

[19] *Hirst, supra,* 15-cr-643 (PKC) Trial Tr. at p.941:6-15.
[20] *Id.* at Trial Tr. at p. 951:9-13.
[21] *Id.* at Trial Tr. at p. 952:4-7.
[22] In *United States v. Hirst*, SFE Flatley even testified about the impossibility of a file content being changed without its file system Modified date being updated. When asked about the Modified date, SFE Flatley said, "It reflects the last time that a change was made to that file and then that file was saved again. So if you were to change something in a file and then not save it, that date would not be touched. **But if you change anything on the file and then save it again, the modified dated will be altered.**" *Id.* at Trial Tr. at p. 942:22-945:2. This statement alone supports nearly all the findings of manual alterations in my Summary of Technical Findings report found at *Raniere, supra,* 18-cr-204-1 (NGG) (VMS) Dkt. 1169-1 at Ex. D.

In addition to demonstrating elsewhere how easy it is to change metadata create dates[23], in this paper I forensically demonstrated that PDF files and JPEG files *name* and *store* the "Create Date" value in same way – inside the content of the file. In his 2016 testimony SFE Flatley not only argued strongly that metadata create dates are *unreliable*, but he also did not waver from this opinion or draw any distinction between metadata create dates in PDF files versus those in JPEG files.

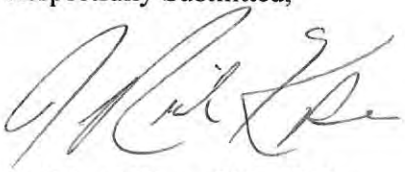
Consider SFE Flatley's expert opinions made under oath:

- SFE Flatley highlighted the similarity between metadata stored inside PDF files and metadata stored inside JPEG files.
- SFE Flatley described two different free tools anyone could use to modify metadata such as EXIF data.
- SFE Flatley declared such tools are easy to obtain from the Web.
- SFE Flatley declared on at least four occasions that metadata create dates are unreliable.
- SFE Flatley described several ways metadata create dates could be altered.
- SFE Flatley declared that the FBI in particular does not rely on metadata creation dates alone to determine when a file was, in fact, created.

To defend SFE Booth's testimony against SFE Flatley's testimony, one may argue that a PDF document is not the same as a JPEG photo. However, to discount SFE Flatley's damning testimony about the unreliability of metadata create dates, one would need to prove that metadata stored inside the content of a JPEG photo file is somehow more reliable than the metadata stored inside the content of a PDF file. It is not. In fact, quite the opposite – It is much easier to modify the EXIF create date of a JPEG file.

Thus, in U.S. vs KEITH RANIERE, there is *no doubt* that the government mischaracterized the reliability of EXIF metadata during trial testimony. No doubt SFE Flatley would agree with that assessment, based on his past testimony, if he were given the opportunity to testify in this case.

Respectfully Submitted,



J. Richard Kiper, PhD, PMP
FBI Special Agent (Retired) and Forensic Examiner

[23] See my Summary of Process Findings report, Appendix A for a full demonstration and debunking the government's claim that EXIF data is "very hard to modify."

Curriculum Vitae of Stephen Michael Bunting

Bunting Digital Forensics, LLC • 33579 Blue Heron Drive • Lewes, DE 19958
Phone: +1.302.260.2633 • E-Mail: stephenbunting@mac.com

Summary of Experience

Mr. Bunting is an experienced digital forensics examiner who is CEO and Senior Forensic Consultant of Bunting Digital Forensics, LLC. He also works as the Senior Manager of Services for SUMURI, LLC as an independent consultant. Formerly Mr. Bunting was a Manager with Alvarez & Marsal (Sept 2012 to Feb 2013) and prior to that a Senior Forensic Consultant with Forward Discovery (Sept 2009 to Sept 2012). (Alvarez and Marsal acquired Forward Discovery in Sept 2012) His responsibilities with Bunting Digital Forensics, Alvarez & Marsal, and Forward Discovery include:

- Acquisition and forensic examination of digital media using industry standard forensics tools;
- Develop & instruct classes on Windows, Macintosh and Mobile Device Forensics;
- Develop & instruct classes on cyber investigations and related course work;
- Investigative consultation and digital forensics examinations in many areas including spoliation, theft of intellectual property, malware analysis, unlawful access of computer systems, theft of corporate resources, employee misuse of computer systems, Medicaid fraud, and support of various types of criminal investigations (prosecution only - no criminal defense work);
- Consult with clients and develop E-Discovery plans;
- Carry out electronic discovery data collection from a wide array of devices and services (servers, network shares, workstations, laptops, smart phones, and cloud services – while Mac is included in the terms workstations and laptops, Mac is a specialty area)
- Under sub-contract (multiple vendors) to the U.S. Department of State, develop & instruct various cyber-based anti-terrorism courses to international law enforcement agencies.
- Under Bunting Digital Forensics, instruct XRY Foundation, Intermediate, PinPoint, XAMN, and Kiosk Courses. Currently the only contract instructor for MSAB (XRY) in the U.S.
- Under Bunting Digital Forensics, instruct courses for Magnet Forensics as a contract instructor.
- Bunting Digital Forensics is under contract to SUMURI, LLC, whereby Steve Bunting manages the services division of SUMURI.

Mr. Bunting retired (August 2009) from a law enforcement career spanning over three decades during which he conducted hundreds of examinations of computer systems for the University of Delaware Police as well as federal, state, and local law enforcement and prosecutorial agencies. He is also a trained and experienced forensic video analyst using the Ocean Systems dTective® and Avid software systems. He is a frequent lecturer and instructor on computer forensics, cyber-crime, and incident response.

Mr. Bunting has testified in many trials as a computer forensics expert. He was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence for receiving the highest test score on his certification examinations. Among his varied certifications he is an EnCase Certified Examiner EnCE (Guidance Software), an AccessData Certified Examiner (ACE), Certified Computer Forensics Technician (HTCN), Certified XRY Instructor, BERLA Certified Vehicle Forensics, Magnet Certified Forensics Examiner, and X1 Social Examiner.

Mr. Bunting is a retired a police captain, having served in the State of Delaware for over thirty-five years. He created and developed the University of Delaware Police Department's Computer Forensic Lab. He has taught computer forensics for Guidance Software, makers of EnCase, and taught as a Lead Instructor at all course levels, including the Expert Series with particular emphasis on "Internet and Email Examinations" course. He has instructed students in computer forensics on an independent study basis for the University of Delaware and is an adjunct faculty member of Goldey-Beacom College, teaching computer forensics. He has been a presenter at several seminars and workshops, the author of numerous "white papers", the principle author of *EnCase Computer Forensics - The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition*, the co-author *Mastering Windows Network Forensics and Investigation* , *the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 2nd Edition,* the co-author *Mastering Windows Network Forensics and Investigation 2nd Edition, the author of EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition* (all published by Wiley).

Recent Consulting Engagements

Mr. Bunting engages in a significant number of instructional / research endeavors as well as engaging in consulting / case work, as one augments the other. Many engagements were totally confidential, while some were public to the extent of the details found in court records. Some of those engagements are described below:

Serving as an embedded mentor with the Albania State Police beginning in 2019 and continuing through 2022, with a contract to continue through 2023. As such, spending two and three week periods, onsite, working with their existing computer forensics lab, enhancing their capabilities, and working with their Counter Terrorism Unit, starting up a brand-new computer forensics lab specific to the CT mission.

Conducted a forensic examination of computers used by a former employee and documented evidence that showed exfiltration of IP data. The exfiltrated data was used to jump start a competing business. The initial report served as a basis to shut down the competing business and bring about a settlement. The former employee did not settle and the matter went to trial, during which Mr. Bunting testified at length concerning the forensics findings.

Recovered data from an Android phone that had been underwater and was delivered 'in pieces'. Using chip-off technique, all data was fully recovered including data that had been deleted.

Served as an expert for two defendants who were facing spoliation claims. Established that opposing expert had failed to discover settings whereby SMS's messages were forwarded from an iPhone to a MacBook Pro. Opposing expert claimed SMS messages were deleted from the iPhone when in fact they were in the opposing expert's possession on the MacBook Pro. Said deletions were offered as evidence of spoliation. Opposing expert also failed to find over 11,000 AIM Messenger chats that were on the iPhone.

Served as a trusted third-party digital forensic examiner in a Virginia case where a former employee was accused of theft of intellectual property, specifically programming code. Determined that accused party provided fabricated exhibits to examine in the form of a contrived MacBook Pro in which the time had been altered to appear to contain historical data when in fact it was only 3 weeks old.

Conducted digital forensics examinations of computers believed to be involved in a telecommunications fraud in the Middle East region, whereby perpetrators were conducting a multimillion-dollar fraud in a balance-transfer scheme exploiting a software defect.

Conducts ongoing training and course development for the U.S Department of State's Anti-Terrorism Assistance Program Cyber Division. As such six to eight courses are delivered each year in varying international locations.

Ongoing consultation with a digital forensics firm that specializes in examinations for copyright infringement cases in the motion picture industry involving peer-to-peer clients to download movies and other protected media.

Ongoing consultation with a digital security company in the UAE, providing incident response support services.

Developed a new Macintosh Digital Forensics course for the Delaware State Police Child Predator Task Force. The course is an in-depth program intended for those with significant digital forensics experience. It includes a unique module entitled "Digging Deeper – Research Techniques to Establish User Culpability", which is the first of it kind.

Developed and delivered a virtual course entitled: Cyber Security Investigations: Incident Response for the FedCTE program. The course was developed for virtual delivery using the AvayaLive virtual classroom and first delivered on June 25, 2014.

Provided expert witness services establishing that the plaintiff fabricated an email submitted during discovery in a civil matter. Testified in US District Court (Princeton, NJ) as expert for defense in computer forensics analysis and email analysis in a hearing to dismiss based on fraudulent documents offered into evidence by plaintiff. Specifically, testified that document

proffered as an email was in fact fabricated to appear as such. – July 09, 2014. The matter is still under litigation.

As a member of a team, conducted an on-site assessment of a major middle east country's governmental cybercrime unit and digital forensics unit, prepared gap analysis reports, and prepared recommendations for creating ISO 17025 compliant laboratory operations, a modern cybercrime investigation and intelligence gathering unit, as well as country-wide expansion of capabilities for both units.

Assigned as principal leak investigator for a major mobile device manufacturer. Investigated significant intellectual property losses on a global basis.

Conducted a security assessment, as part of a team, of a Caribbean country's government IT infrastructure and made recommendations for securing their systems according to best practices.

Conducted computer forensic examination of all computers from a dental practice in a Medicaid fraud case. Examination involved reconstruction of a dental practice's business transactions spanning several years through analysis of SQL transaction logs from Patterson's *Eaglesoft* dental practice software. The findings in the report submitted substantiated ongoing fraud and induced a guilty plea, resulting in the incarceration of the offending dentist.

Conducted computer forensic examination of over two-dozen laptops belonging to employees of a major brand integrity unit, which investigates and mitigates brand piracy for its parent company. The unit was distributed in six countries and had been accused of various breaches of duty and unlawful acts. The examination took several months to complete and findings documented and substantiated the majority of the allegations, resulting in the dismissal of several employees.

Certifications

X1 Social Examiner	April 2019
Magnet Certified Forensics Examiner	March 2018
BERLA Certified Vehicle Forensics	September 2017
Certified XRY Instructor, MSAB (Sweden)	October 2013
Certified ACE AccessData Certified Examiner	April 2011
Certified iPhone Examiner, MSAB	November 2010
Certified XRY Complete Examiner, MSAB	October 2010
Certified LAW PreDiscovery Administrator, LexisNexis	January 2010
Certified LAW PreDisovery User, LexisNexis	January 2010

Certified Computer Forensic Technician, High Tech Crime Network	September 2001
EnCase Certified Examiner, Guidance Software	April 2002
Certified Cell Phone Examiner, Paraben Corporation,	May 2005
Certified PDA Examiner, Paraben Corporation	May 2005
State of Delaware Council on Police Training Certified Police Officer	April 1975

Employment History

SUMURI, LLC – Camden, DE – Senior Manager of Services (as independent contractor) – November 2016 to present

- Provide management services for SUMURI's Services Division
- Develop and carry out the business plan for services
- Coordinate services, match resources with service needs, and ensure quality control
- Conduct digital forensic examinations and investigations

Bunting Digital Forensics, LLC – Lewes, DE – CEO & Senior Digital Forensic Consultant – February 2013 to present

- Conduct digital forensics examinations on a variety of media, including mobile devices
- Develop training programs for various cyber related topics
- Deliver training programs as an independent contractor for the Antiterrorism Assistance Program Cyber Division (see NDI below)
- Conduct assessments of digital forensics laboratories, conduct a gap analysis, and recommend a roadmap for improvements leading to accreditation
- Conduct specialized digital forensics examinations in support of Medicaid fraud cases

Microsystemation (MSAB) – Stockholm, Sweden – Contract instructor for XRY training courses – October 2013 to present

Teach XRY Mobile Device Forensic Solutions Courses

Alvarez and Marsal, Washington, DC – Manager, Forensic Technology Services – September 2013 to February 2013

- Develop and deliver a variety of training courses, including Macintosh Forensics, Incident Response, and Advanced Digital Forensics Courses.
- Developed and facilitated a table top training exercise to test and enhance the incident response capabilities of a large web hosting company
- Conduct digital forensic examinations on media associated with compromised systems.

• Interim Management, specifically Principle Leak Investigator for a large telecommunications company experiencing a significant loss of intellectual property.

Forward Discovery, Inc – San Antonio, TX – Senior Forensic Consultant – September 2009 to September 2012

Information security company that provides digital investigation, electronic discovery, vulnerability assessments and training services to corporate and government clients.

• Acquisition and forensic examination of digital media using industry standard forensics tools

• Develop & Instruct classes on Windows, Macintosh and Mobile Device Forensics

• Develop & Instruct classes on Cyber Investigations and related course work

• Investigative consultation in areas including theft of intellectual property, malware analysis, unlawful access of computer systems, theft of corporate resources, employee misuse of computer systems, and support of various types of criminal investigations (prosecution only - no criminal defense work).

• Consult with clients and develop E-Discovery plans

• Carry out electronic discovery processing from initial acquisition to final load file

Network Designs, Inc. – McLean, VA – Senior Instructor ATA Cyber Division as an Independent Contractor – September 2009 to present. On a contract basis to NDI, work as a Senior Instructor supporting the U.S Department of State Anti-Terrorism Assistance Program's Cyber Division, which included the following:

• Develop training modules for new training programs

• Provide advisement, briefings and presentations to foreign law enforcement officers on areas including cyber terrorism and cyber crime

• Provide technical computer investigation training to law enforcement and governmental agencies worldwide. Course taught include: Identification & Seizure of Digital Evidence, Introduction to Digital Forensics & Investigations, Macintosh Forensics, Cell Phone Forensics Consultation, EnCase Software Consultation, Server Incident Response (ADFC), Fundamentals of Network Security, Cyber Unit Management Consultation Proactive Internet Investigations Course, Forensic Equipment Grant Consultation, and Digital Forensic Lab Mentoring and Consulting.

Guidance Software – Pasadena, CA – Part-time Instructor - 2004 - 2005.

- Lead instructor teaching courses at all levels (Beginning to Expert)
- Assisted in course development and review

University of Delaware Police Department – Newark DE – Captain - July 1980 to August 2009.
Principle duties were:

- Computer Forensics Unit (Founded and Managed)
- Accreditation (Accreditation Manager)
- Southern Operations (Managed)

Education

University of Delaware - Computer Applications Certificate – Concentration in Network Environments - August 2004

Wilmington College - Bachelor of Science Applied Professions / Business Management - May 1986

Delaware Technical and Community College - 52 credit hours in the Criminal Justice Program

University of Delaware - Associate in Art - May 1973

Publications

How Did That Photo Get On That iPhone? Deep Dive Into The iOS "Photos.sqlite" database: Part 1 **– MSAB Blog – (to be published) Fall 2022**

Forensic Analysis of Spoliation and Other Discovery Violations - Part 2 of a 2-Part Series - Windows Examinations - eForensics Magazine - December 2016

Forensic Analysis of Spoliation and Other Discovery Violations **- Part 1 of a 2-Part Series - Macintosh Examinations - eForensics Magazine - October 2016**

EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide**, 3rd Edition - author - Wiley - September 2012**

Mastering Windows Network Forensics and Investigation **(one of four co-authors) - Wiley - 2012**

EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide**, 2nd Edition - author - Wiley - November 2007**

Mastering Windows Network Forensics and Investigation **(one of two co-authors) - Wiley - April 2007**

Encase Computer Forensics—The Official EnCE: Encase Certified Examiner Study Guide **- primary author - Wiley - January 2006**

Memberships and Affiliations

Infragard – secure member of the Wilmington, Delaware Chapter since June 2004.

High Technology Crime Investigation Association - member since August 2002.

High Tech Crime Network - member from September 2001 to date.

National White Collar Crime Center - designated agency contact person for agency membership in the organization - January 2001 to 2009.

Courses Recently Developed

Chip-off / JTAG Bootcamp – A two-day course intended for stand-alone or to supplement a forensic software course. A pilot was recently delivered in January 2017.

Macintosh Digital Forensics – A new course for delivery by Bunting Digital Forensics to various clients. August 2015.

Cyber Security Investigations: Incident Response – New course development and delivery (part of two-person teams) – course was created for virtually delivery using the AvayaLive virtual classroom, with first delivery on June 25, 2014.

Mastering Macintosh Forensics – Rewrite (part of a four-person team) – Alvarez & Marsal for U.S. Department of State ATA – February 2013 – March 2013

Introduction to Digital Forensics and Investigation - Rewrite (part of two-person team) - U.S. Department of State ATA (Humtech) May 2012 - January 2013

Windows Server Incident Response - New course (part of two-person team) - Organization of American States May 2012 - Sept 2012

Advanced Digital Forensics Consultation (Windows / Linux / Macintosh Server Incident Response), New course (solo assignment) plus developed and built portable server lab -U.S. Department of State ATA - Sept 2011 - March 2012

Mastering Macintosh Forensics - New course (solo assignment) - U.S. Department of State ATA - Jan - June 2011

Languages

Primary language is English, however during last several years have spent considerable time teaching and consulting in Latin American countries through interpreters, during which some Spanish skills have been acquired. Currently have the ability and experience demonstrating, teaching, and using EnCase and XRY software using the Spanish interface.

Teaching and Presentation Experience

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, May 9 - 20, 2022, Tirana, Albania (Split - Onsite Delivery / Virtual Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Apr 11 - 22, 2022, Tirana, Albania (Onsite Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Mar 7 - 18, 2022, Tirana, Albania (Onsite Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Jan 10 - 21, 2022, Tirana, Albania (Onsite Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Nov 1 - 19, 2021, Tirana, Albania (Onsite Delivery)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Sept 6 - 24, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, May 28 – June 14, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, May 10 - 28, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Apr 5 - 23, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Feb 22 - Mar 12, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Jan11 - 29, 2021, Tirana, Albania (Delivered Virtually)

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Feb 24 - Mar 13, 2020, Tirana, Albania

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Jan 13 - 24, 2020, Tirana, Albania

Digital Forensics Equipment Grant and Consultation - U.S. Department of State ATA, Nov 11 - 22, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Sep 9 - 20, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Jun 20 - Jul 5, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Apr 30 - May 17, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Feb 28 - Mar 22, 2019, Tirana, Albania

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Sept 3 – 14, 2018, Beirut, Lebanon.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Aug 6 – 10, 2018, Naperville, IL.

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, July 23 – Aug 3, 2018, Beirut, Lebanon.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – June 18 – 22, 2018, Naperville, IL.

Magnet AXIOM Forensics Course (Online) -Magnet Forensics - Apr. 24-27 2018

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Dec 11-15, 2017, Nigerian MOI in Dubai, UAE.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Nov 27- Dec 1, 2017, Nokesville, VA.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Aug 21-25, 2017, Lansing, MI.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Mar 6-10, 2017, Singapore.

Chip-off Forensics Bootcamp – Sumuri, LLC – January 30, 2017, Dover, DE.

Foundation, Intermediate, XAMN XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 24-28, 2016, Nairobi, Kenya.

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, July 18 - 29, 2016, Shillong, Meghalaya - India.

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – July 6-15, 2016 – Shillong, Meghalaya – India.

Foundation XRY Mobile Phone Forensics – Micro Systemation, A.B. – May 16-17, 2016, U.S. Secret Service National Computer Forensics Institute Hoover, AL.

Foundation and Intermediate XRY Mobile Phone Forensics (private course for 5 members of the Kingdom of Saudi Arabia Ministry of the Interior) – Micro Systemation, A.B. – May 9-13, 2016, London, UK.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Feb 22-26, 2016, Jakarta, Indonesia.

Mobile Device Forensics Consultation, U.S. Department of State ATA, Feb 8-19, 2016, Jakarta, Indonesia.

Foundation & Kiosk XRY Mobile Phone Forensics - Micro Systemation, A.B. – Feb 2-4, 2016 – Singapore

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 21-25, 2015 – Washington, DC

Proactive Internet Investigations Course - U.S. Department of State ATA – Aug 10 - 21, 2015 – Mexico City, Mexico

EnCase Transition Training, Bunting Digital Forensics Custom Course, May 26 – 27, 2015 Delaware State Police Child Predator Task Force, Dover, DE

Foundation and Intermediate XRY Mobile Phone Forensics (private course for 5 members of the Kingdom of Saudi Arabia Ministry of the Interior) – Micro Systemation, A.B. – May 18-22, 2015 – New York, NY

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, May 3 - 14, 2015, Muscat, Oman

EnCase I (Guidance Software Course - ATP) – Abu Dhabi Police Department – Mar 1 – Mar 5, 2015 – Abu Dhabi, United Arab Emirates

Proactive Internet Investigations Course - U.S. Department of State ATA – Jan 26 - Feb 6, 2015 – Cuernavaca, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Jan 16-23, 2015 – Cuernavaca, Mexico

Proactive Internet Investigations Course - U.S. Department of State ATA – Nov 17 - 28, 2014 – Tijuana, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Nov 6-14, 2014 – Tijuana, Mexico

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 20-24, 2014 – Alexandria, VA

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Sep 22-26, 2014 – Santiago, Chile

Proactive Internet Investigations Course – U.S. Department of State ATA – August 11 – 22, 2014 – Ciudad de México, México

Digital Forensic Lab Mentoring and Consulting – Lead Instructor - U.S. Department of State ATA, July 14 – 25, 2014, Medellin & Bucaramanga, Colombia

Cyber Security Investigations: Incident Response – U.S. Department of State FedCTE Program – June 24, 2014, Virtual Class - AvayaLive

Digital Forensic Lab Mentoring and Consulting – Lead Instructor U.S. Department of State ATA, May 5 – 16, 2014, Cali & Pereira, Colombia

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Mar 24 – Apr 4, 2014, Bogota, Colombia

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Apr 7-11, 2014 – Alexandria, VA

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Mar 3-7, 2014 – Vancouver, BC

Proactive Internet Investigations Course - Lead Instructor - U.S. Department of State ATA – Jan 27 – Feb 7, 2014 – Cuidad Juarez, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Jan 20-25, 2014 – Cuidad Juarez, Mexico

Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Nov 20-22, 2013 – San Diego, CA

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Nov 4-9, 2013 – Chihuahua, Mexico

Computer Forensics for Legal Professionals, September 24, 2013, Widener University School of Law, Wilmington, DE

Introduction to Digital Forensics and Investigation - Lead Instructor - U.S. Department of State ATA, September 2-13, 2013, Mexico City, Mexico

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, July 15-26, 2013, Dakar, Senegal

Introduction to Digital Forensics and Investigation (New Version Pilot) - Lead Instructor - U.S. Department of State ATA, April 8-19, 2013, Manila, Philippines

Identification & Seizure of Digital Evidence - Lead Instructor - U.S. Department of State ATA – Mar 9-17, 2013 – Muscat, Oman

Identification & Seizure of Digital Evidence - U.S. Department of State ATA - Feb 11-21, 2013 - Dakar, Senegal

Mastering Macintosh Forensics, Alvarez & Marsal, Oct 29 - Nov 2, 2012, 2012, Washington, DC

Incident Response Tabletop Exercise, large web hosting client, Oct 16-17, 2012, San Antonio, TX

Macintosh Incident Response, HTCIA, Sept 16-19, 2012, Hershey, PA

Windows Server Incident Response - Lead Instructor - Organization of American States, Sept 3-7, 2012, Trinidad & Tobago

Fundamentals of Network Security, U.S. Department of State ATA, July 23 - Aug 3, 2012, Bogota, Colombia

Introduction to Digital Forensics and Investigation (Pilot for revised program) - U.S. Department of State ATA, April 23 - May 4, 2012, Mexico City, Mexico

Mastering Macintosh Forensics, Ocean County Prosecutor's Office, April 16-20, 2012, Tom's River, NJ

Advanced Digital Forensics Consultation (Windows / Linux / Macintosh Server Incident Response), Developer and Lead Instructor - U.S. Department of State ATA Mar 5-16, 2012, Bogota, Colombia

Cyber Unit Management Consultation, U.S. Department of State ATA, Sept 5-16, 2011, Bogota, Colombia

Cell Phone Forensics Consultation, U.S. Department of State ATA, July 11-22, 2011, Antigua.

Macintosh Forensics & Advanced Forensics Consultation, Developer and Lead Instructor - U.S. Department of State ATA, June 6-17, 2011, Bogota, Colombia.

Forensic Equipment Grant Consultation, U.S. Department of State ATA, May 17-31, 2011, Bangkok, Thailand

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, May 2-13, 2011, Mauritius

Advanced Forensic Acquisition & Analysis - Delaware ICAC - March 21-25, 2011, Dover, DE

Forensic Acquisition & Analysis - Delaware ICAC- Feb 21-25, 2011, Dover, DE

Cyberbullying - Cape Henlopen High School - January 27, 2011, Lewes, DE

Software Consultation: EnCase 1 & EnCase 2, U.S. Department of State ATA, Jan 10-21, 2011, Bangkok, Thailand

Incident Response & Forensic Tools Overview - Delaware Cyber Terrorism Exercise, Oct 27, 2010, Smyrna, DE

Identification & Seizure of Digital Evidence - U.S. Department of State ATA - June 3 - 11, 2010 - Mexico City, MX

EnCase Computer Forensics I – Lead Instructor - North Carolina ICAC- April 26 - 30, 2010 - Raleigh - Durham, NC

EnCase Computer Forensics II – Lead Instructor - Sidley Austin LLP - February 22 - 25, 2010 - Chicago, IL

EnCase Computer Forensics I - Qatar National Bank - October 11 - 15, 2009 - Doha, Qatar

EnCase Computer Forensics I - Abu Dhabi Police Department - October 4 - 8, 2009 - Abu Dhabi, UAE

Introduction to Computer Forensics - University of Delaware Police - August 17-21, 2009 - Lewes, DE

Advanced Computer Forensics Techniques - Computer Forensics Analysis and Training Center - June 4-5, 2009 - Sharon Hill, PA.

Cyberbullying - May 11, 2009 - Long Neck Elementary School - Millsboro, DE

"Computer Forensics - Current State and Future Challenges" - Computer Crimes Colloquium - April 7, 2009 - Wilmington University - Dover, DE

Identity Theft - City of Lewes Neighborhood Watch Meeting - March 23, 2009 - Lewes, DE

Disaster Recovery (CIS 486) - Goldey-Beacom College - January to March 2008 - Wilmington, DE.

Forensic Acquisition and Analysis - November 16-20, 2008, Dubai Police Department, Dubai, UAE

Cyber Stalking - Delaware Domestic Violence Council - Dover Police Department, November 7, 2008, Dover, DE

Computer Forensics (CIS 362) - Goldey-Beacom College - October to December 2008 - Wilmington, DE.

Advanced Computer Forensics - September 22-26, 2008, Sidley - Austin in Chicago, IL

Computer Forensics Primer for the Press - September 17, 2008 - Delaware Valley Press Club - Chester, PA.

Investigation Crimes Involving Computers - August 28-29, 2008 - Newark, DE.

Introduction to Computer Forensics - Computer Forensics and Analysis Training Center - August 26-27, 2008 - Sharon Hill, PA.

Disaster Recovery (CIS 486) - Goldey-Beacom College - March to April 2008 - Wilmington, DE.

Computer Forensics (CIS 362) - Goldey-Beacom College - October to December 2007 - Wilmington, DE.

Computer Forensics for Medical / Legal Professionals - University of Delaware Special Programs - November 9, 2007

Windows Network Investigations and Forensics - HTCIA Regional Training - June 19, 2007 - Newark, DE

User Services - First Response to Crime Scenes Workshop - Special Interest Group on University and College Computing Services - Edmonton, Canada - November 5, 2006

Cyber Stalking - Delaware Domestic Violence Council - November 16, 2006 - Dover, DE.

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 28, 2006 - Dewey Beach, DE.

CyberSpeak Podcast - Microsoft Log Parser Forensic Applications - June 3, 2006

CyberSpeak Podcast - User Assist Registry Key and Restore Point Forensics - May 13, 2006

Investigation of Cyber Incidents - University of Delaware System Administrators Group - May 17, 2006 - Newark, DE

Identity Theft and Cyber Safety - DuPont Experimental Station Staff - March 14, 2006 - Wilmington, DE.

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 22, 2005 - Lewes, DE.

First Response Issues for Crimes Involving Computers - Hosted by the U.S. Attorney's Office - September 16, 2005 - Dover, DE.

Examination of Photoshop Layer Data - RCFG GMU 2005 - August 15 & 18, 2005 - Fairfax, VA

Cyber-sabotage, Espionage, & Other Security Threats, February 23, 2005, Lorman Education Services, Newark, DE

Computer Forensics in the Courtroom, January 7, 2005, Widener University School of Law, Wilmington, DE

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 30 - October 1, 2004 - Dewey Beach, DE.

Forensic Examination of Peer-to-Peer Client Software Artifacts -NJSP High Tech Crime Unit. September 22, 2004, Trenton, NJ.

Introductory Computer Forensics Guidance Software - Sterling, VA Jun 29 - Jul 2, 2004 (32 hrs) Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Jun 22 - 25, 2004 (32 hrs) Lead Instructor

Email Examinations Lab at CEIC 2004 Myrtle Beach, SC Jun 6 - 9, 2004 (7.5 hrs - five presentations) Lead Instructor

Photoshop Layer Metadata Examinations CEIC 2004 Myrtle Beach, SC Jun 8, 2004 (1.5 hrs) Lead Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Apr 27 - 30, 2004 (32 hrs) Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Mar 30 - Apr 2, 2004 (32 hrs) Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Feb 3-6, 2004 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Jan 6-9, 2004 (32 hrs) Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Nov 18-21, 2003 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Oct 21-24, 2003 (32 hrs) Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA Sept 9-12, 2003 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Aug 12-15, 2003 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA July 8-11, 2003 (32 hrs) Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA June 17-20, 2003 (32 hrs) Instructor

Internet / Email Guidance Software - Sterling, VA May 6-9, 2003 (32 hrs) Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA Mar 4-7, 2003 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Feb 25-28, 2003 (32 hrs) Instructor

Internet Safety for Children - Winter / Spring 2003 semester offering through the University of Delaware Continuing Education Division

Cyber-Stalking and Related Crimes Involving Computers: October 7, 2002 in Newark, DE.

Computer Crime Issues for Prosecutors: - Presented to the Wicomico County States Attorney's Office (4/20/01) and to the Attorney General's Office for the State of Delaware Sex Crimes Unit (10/4/02).

Computer Forensics: - during the spring semester 2002, supervised and directed an independent course of study in computer forensics for a University of Delaware senior majoring in computer science. Program was under the auspices of Professor Chien-Chung Shen. Student is now employed with Price, Waterhouse, Cooper in the computer forensics division.

The Internet as an Investigative Tool: Presented at the University of Delaware (5 presentations: 12/5/00, 1/8/01, 8/6/01, 8/13/01, & 8/26-27/02), at the Eastern Shore Criminal Justice Academy (3 presentations: 2/16/01, 3/8/01, and 3/20/01), and at Mount St. Mary's College (6/26/02).

Computer Crimes: 1st Responder Issues - course developed and presented to the University of Delaware Police as a 2-hour block during in-service training. Presented May 31, 2001, June 7, 2001, May 30, 2002, and June 5, 2002.

Training Courses Completed

Counterterrorism Assistance Planning Event	U.S. Dept of State – Oct 19 – Nov 4, 2022 Virtual
Magnet Forensics Virtual Summit 2020	Magnet Forensics – May 4 – 29, 2020 Virtual
XRY Train-the-Trainer Training	MSAB – Aug 19– 23, 2019 Stockholm, SE
X1 Social Discovery	Digital Shield – April 9-11, 2019 Online
XRY Train-the-Trainer Training	MSAB – Aug 23–26, 2018 Washington, DE
HTCIA Conference	HTCIA – Aug 19-22, 2018 Washington, DC
AX300 – AXIOM Advanced Mobile Examinations	Magnet Forensics – Oct 24-27, 2017 Sterling, VA
iVE Vehicle Forensics	Berla – Sep 25-29, 2017 Annapolis, MD
AX200 - AXIOM Examinations	Magnet Forensics – Sep 19-22, 2017 Online
XRY Train-the-Trainer Training	MSAB – Aug 30– Sep 1, 2017 Stockholm, SE
XRY Version 7 Training	MSAB – Aug 22–26, 2016 Stockholm, Sweden
XRY Version 7 Training	MSAB – Mar 28–Apr 1, 2016 Stockholm, Sweden
XRY Advanced Acquisitions	MSAB – Mar 21 – 25, 2016 Freehold, NJ
XRY Advanced Applications Analysis	MSAB – Dec 14 – 18, 2015 Washington, DC

XRY Train-the-Trainer Annual Training	MSAB – Sept 7-11, 2015 Stockholm, Sweden
XRY Train-the-Trainer Course	MSAB – Sept 30- Oct 11, 2013 Stockholm, Sweden
FTK Bootcamp Version 3	Access Data - April 5-7, 2011 - Online
XRY Physical Acquisition & Analysis Training	MSAB - Oct 6-8, 2010 - Alexandria, VA
XRY Logical Acquisition & Analysis Training	MSAB - Oct 4-5, 2010 - Alexandria, VA
Basic Malware Analysis	HB Gary - April 20-21, 2010 - Columbia, MD
LAW PreDiscovery Certified Administrator Course	LexisNexis - Jan 14, 2010 - Washington, D.C.
LAW PreDiscovery EDD Certified User Course	LexisNexis - Jan 12-13, 2010 - Washington, D.C
Microsoft Exchange Server 2007	Global Knowledge - Jan 26 - 30, 2009 - Arlington, VA
HTCIA Conference (24 hrs)	High Tech Crime Investigator's Association - Oct 20-22, 2008, Atlantic City, NJ
Operation Fair Play (40 hrs)	Delaware State Police ICAC – Wyoming Tool Kit Training - Mar 31-Apr 4, 2008, Dover, DE
Neutrino Cell Phone Forensics (16 hrs)	Guidance Software - January 15 – 16, 2008, Sterling, VA.
Macintosh Forensics (40 hrs)	Phoenix Data Group - October 15-19, 2007 - Sharon Hill, PA
Vista Forensics	Access Data - July 20, 2007 - Washington, DC
Advanced Windows Intrusion Investigator's Course (40 hrs)	SYTEX - February 27 – March 3, 2006, FBI Academy, Quantico, VA
Adobe Photoshop for Forensic Video Analysts (16 hrs)	Resolution Video - December 14-15, 2005 - Reston, VA
Regional Computer Forensics Group Seminar (40 hrs)	RCFG / HTCIA - August 15-19, 2005 - GMU - Fairfax, VA.
Cell Seizure (16 hrs)	Paraben - May 18-19, 2005 in Newark, DE
PDA Seizure (16 hrs)	Paraben - May 16-17, 2005 in Newark, DE

Enterprise Security & Vulnerability (36 hrs)	USSS / SEARCH - April 18-22, 2005 in Cherry Hill, NJ
Access Data FTK Advanced Internet Training Course (24 hrs)	Access Data - March 15 – 17, 2005 in Dover, DE.
Ocean Systems: dTective (Advanced Video Forensic Analysis) (16 hrs)	Ocean Systems - Feb. 24 – 25, 2005 in Burtonsville, MD.
Advanced UNIX Investigator's Course (40 hrs)	SYTEX - December 6 – 10, 2004, Ellicott City, MD.
EnCase EnScript Programming (32 hrs)	Guidance Software - November 16 – 19, 2004, Sterling, VA.
Networks and Networking for Agents / System Security and Exploitation (80 hrs)	SYTEX - October 18 – 29, 2004, Ellicott City, MD.
Law Enforcement Video Association Annual Training Conference 2004 (16 hrs)	LEVA - October 6 – 7, 2004 Washington, D.C.
NIJ Law Enforcement Technology Institute 2004 (40 hrs)	NIJ - July 11 – 16, 2004, Washington, D.C.
Computer and Enterprise Investigations Conference / TechnoSecurity Conference 2004 (28 hrs)	Guidance Software - June 6 – 9, 2004 in Myrtle Beach, SC.
Ocean Systems: dTective (Advanced Video Forensic Analysis) (16 hrs)	Ocean Systems - May 6 – 7, 2004 in Burtonsville, MD.
Ocean Systems: Introduction to Forensic Video Examinations (24 hrs)	Ocean Systems - May 3 – 5, 2004 in Burtonsville, MD.
Access Data FTK Intermediate Training Course (24 hrs)	Access Data - April 5 – 7, 2004 in Dover, DE.
EnCase Expert Series: Internet & Email Examinations (32 hrs)	Guidance Software - February 4 - 7, 2003 in Sterling, VA.
EnCase Advanced Computer Forensics (32 hrs)	Guidance Software - January 21- 24, 2002 in Sterling, VA.
Introduction to Programming Concepts (Visual Basic 6) (50 hrs)	University of Delaware Course - Wilm, DE – Fall 2002
Computer and Enterprise Investigations Conference 2002 (16 hrs)	Guidance Software - September 16-17, 2002 Chantilly, VA.

Regional Computer Forensics Group Seminar (40 hrs)	RCFG / HTCIA - August 12-16, 2002 - GMU - Fairfax, VA.
ILook Computer Forensics Software (24 hrs)	ACES / FBI / IRS / NCFS - July 23-25, 2002 Orlando, FL.
Firewalls and Virtual Private Networks (16 hrs)	CSI / NIPC / FBI - May 22-23, 2002 MSP - Columbia, MD.
Internet Investigations and Child Exploitation Overview (8 hrs)	SEARCH - April 6, 2002, CCU - Conway, SC.
Techno-Security 2002 Conference (28 hrs)	The Training Company - April 7-10, 2002 - Myrtle Beach, SC
Enterprise Networks (50 hrs)	University of Delaware - Wilm, DE - Spring 2002
EnCase Advanced Computer Forensics (32 hrs)	Guidance Software - February 19-22, 2002 - Leesburg, VA.
LAN (Local Area Networks) (50 hrs)	University of Delaware - Newark, DE - Fall 2001
EnCase Intermediate Computer Forensics (32 hrs)	Guidance Software - August 7-10, 2001 - Leesburg, VA .
Techno-Security 2001 Conference (28 hrs)	The Training Company April 22-25, 2001 - Myrtle Beach, SC
WAN (Wide Area Networks) (50 hrs)	University of Delaware - Newark, DE - Spring 2001
Advanced Data Recovery and Analysis Course (40 hrs)	NW3C - October 23-27, 2000 - Fairmont, WV.
The Internet as in Investigative Tool (8 hrs)	NW3C / IFCC - October 12, 2000 - Fairmont, WV.
Basic Data Recovery and Analysis Course (40 hrs)	NW3C July 24-28, 2000 in Myrtle Beach, SC.

Computer Forensics Expert Witness Experience

STRIKE 3 HOLDINGS, LLC v. JOHN DOE SUBSCRIBER ASSIGNED IP ADDRESS 68.83.56.212 and STRIKE 3 HOLDINGS, LLC v. JOHN DOE INFRINGER INDENTIFIED AS USING IP ADDRESS 69.113.113.228 – U.S. District Court of New Jersey in Camden – Testified at two hearings, May 31, 2019 and July 23, 2019, regarding the function of peer-to-peer bittorrent software, detecting

copyright infringers, and basics of networking and IP addresses on behalf of the plaintiff alleging copyright infringement using bittorrent software to download protected works.

Deposed on April 1o, 2019 in Georgetown, DE in the matter of LendUS, LLC vs John Goede & John Schrenkel (C.A. No. 2018-0233-SG), on behalf of the plaintiff. Defendant claims text messages on his phone were deleted when plaintiff caused Verizon to suspend his telephone service and thus the plaintiff's actions precluded the defendant from complying with discovery request to produce said messages. Testified and demonstrated that cutting off from service does not delete messages, as messages are stored on the iPhone proper.

Laser Tone Business Systems, LLC vs Delaware Micro-Computer, PrintIT Solutions, Alex J. Farling, and Justin McGinnis (CA No. 2017-0429-TMR). On behalf of plaintiff, conducted a forensic examination of computers used by McGinnis and documented evidence that showed exfiltration of IP data. The exfiltrated data was used to jump start a competing business. The initial report served as a basis to shut down the competing business and bring about a settlement. McGinnis did not settle and the matter went to trial, during which Mr. Bunting testified at deposition (August 15, 2018) and later at trial (December 6, 2019) concerning the forensics findings. As of 4/13/19, the judge has not yet rendered a decision in the case.

Crawford and Company v Larry W. Daniel and Cunningham Lindsey Claims Management, Inc Civil Case No 17-1-01244 – Superior Court of Cobb County State of Georgia – Submitted affidavit on September 12, 2017 on behalf of Crawford that an iPhone submitted by the defendant as part of electronic discovery had the messages set to delete after 30 days and that the user has enabled backup encryption, thereby preventing the contents from being acquired. Case settled without going to trial.

AdMarketer, LLC and Credit Benefit Services, LLC v Isaac "Zack" Bernato; Dennis H. James; CRM Holding Company, LLC; IMT Marketplace, LLC; World Clicks, LLC; and Valerie DiNardo – Civil Action File No: 2015CV267337 in the Superior Court of Fulton County State of Georgia – Submitted affidavit on March 31, 2017 on behalf of the defendant that opposing expert had made a finding that defendant had deleted messages, thus supporting a spoliation claim. Affidavit stated that opposing expert had not discovered iPhone message setting for 'delete after 30 days' nor had he discovered that SMS forwarding was enabled, enabled specifically to a Mac laptop that was in the possession of the opposing expert and which opposing expert had failed to examine. This laptop contained all the chat messages that the expert claimed were deleted. Further the affidavit stated that the opposing expert had used only one tool in his examination and in doing so missed over 11,000 AIM messages, many of which were relevant to the case. Defendants filed bankruptcy and case settled without trial.

Tamika Covington vs International Association of Approved Basketball Officials, Board 193, et al. (CIVIL ACTION NO. 3:08-cv-03639) - US District Court (Princeton, NJ) – Testified as expert for defense in computer forensics analysis and email analysis in a hearing to dismiss based on fraudulent documents offered into evidence by plaintiff. Specifically, testified that document proffered as an email was in fact fabricated to appear as such. – July 09, 2014.

Network Computing Services Corporation vs Haynsworth, Sinkler, P.A. Belton T. Zeigler and John Tiller (South Carolina) – Submitted two affidavits for the plaintiff regarding deleted emails in a case alleging legal malpractice – April 2010

State of Delaware vs Irina Malinovskaya (3rd trial - Murder 1st) – Testified as computer forensics expert regarding analysis of defendant's computer. Also testified that an email offered by the defendant after the 2nd trial was fabricated and offered as evidence. The defendant was convicted of tampering with physical evidence. - 2007

Cpl B. Kurt Price et al. vs Colonel L. Aaron Chaffinch et al. (US District Court) Submitted affidavit as to wiping of a hard drive by the plaintiff - May 2006

State of Delaware vs Irina Malinovskaya (2nd trial - Murder 1st) Testified - 2006

State of Delaware vs Stephanie McMullen (Munchausen's Nurse case) Testified - 2006

State of Delaware vs Eric Kemske (Manufacture, distribute, possess child pornography – peer-to-peer software involved) – Testified - 2005

State of Delaware vs Keith Appleby (Suppression Hearing - Computer Intrusion Case) Testified - 2003

EXHIBIT B

FIAT JUSTITIA RUAT CAELUM

TULLY & WEISS
RETIRED
ATTORNEYS AT LAW

March 16, 2022

VIA EMAIL
Assistant United States Attorney Tanya Hajjar
U.S. Attorney's Office
Eastern District of New York
271 Cadman Plaza East
Brooklyn, NY 11201
Tanya.hajjar@usdoj.gov

Re: *United States v. Keith Raniere*, 18-CR-204 (NGG)

Dear AUSA Hajjar:

This letter is submitted on behalf of defendant Keith Raniere in the above-entitled case and pursuant to Rule 16 of the Federal Rules of Criminal Procedure, *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and *Kyles v. Whitley*, 514 U.S. 419 (1995). Mr. Raniere demands the following information, documents, and other materials based on newly discovered evidence that was uncovered following trial, sentencing, and appellate briefing in this case. Each below demand is supported by a specific finding made after the trial and sentencing of Mr. Raniere, which in turn, led to the discovery that the government either possesses additional information or materials related to these findings or should have been aware of same.

Firstly, we request information pertaining to photographic images that were purportedly taken in 2005 depicting underage nudity on a camera's CF card and hard drive that were seized from 8 Hale Drive on March 27, 2018. As the government is aware, the dates of these photographs were crucial to establishing the age of the individuals at the time the photographs were taken during jury trial. Mr. Raniere concludes that the above-mentioned evidence was manipulated and materially altered while in FBI custody.

Secondly, we request information pertaining to witness collusion and tampering between key witnesses, namely, Nicole and Daniela. Considering the newly discovered evidence on this issue, we also seek information concerning other witnesses and potential government tampering.

Thirdly, we request information concerning dates, times, and other documentary proof of Nicole's travels.

Lastly, we request information pertaining to the arrest of Mr. Raniere in Mexico.

Even if the government were unaware of the below issues, they constitute newly discovered evidence pursuant to Rule 33 of the Federal Rules of Criminal Procedure. Therefore, we request production of the following:

Camera Images and Data

FRESNO
1340 VAN NESS
(559) 321-0907
LOS ANGELES
220 S. PCH, STE 106
(424) 383-9700
MARTINEZ
713 MAIN ST.
(925) 229-9700
REDDING
1388 COURT ST., STE G
(530) 999-9700
SAN FRANCISCO
333 WEST PORTAL, STE A
(415) 360 9007
SELMA
1916 E. FRONT ST.
(559) 860-0970

1. The entire chain of custody of the seized camera, camera's CF card, and hard drive since its seizure on March 27, 2018, including every individual that had possession or control of these items along with specific dates as to when the evidence was in possession and when the chain of custody was broken as well as for any derivative evidence copies that were made.[1]
2. CART evidence receipts for all devices seized from 8 Hale Drive on March 27, 2018.
3. Documentation establishing exactly when, and the circumstance as to why, photographs were manually added to the camera's CF card between April 11, 2019 and June 11, 2019, while in FBI custody. Specifically, this request relates to the disparity between the two Forensic Toolkit reports produced on these dates and why new files appeared on the latter report.
4. The identity of the individual(s) who accessed the camera's CF card on September 19, 2018 and altered the file system dates while in the custody of the FBI. According to the camera's CF card's file listing, the accessed dates for all active files were changed to September 19, 2018, indicating that the dates were altered on at least this one occasion during the six months they were in the custody of the FBI. We further request the true and original dates that were indicated prior to alteration.
5. The identity of the individual(s) who altered the dates of the photographs through manual intervention and the dates on which the alterations occurred. Specifically, this request refers to the differences in dates between the EXIF dates and Modified dates.
6. The identity of the individuals(s) who manually altered the modified date on the photograph identified as IMG_0175. Alteration is evidenced by the fact that the EXIF CreatorTool value of said image is set to "Adobe Photoshop Elements 3.0," indicating Photoshop was used to open and modify the file data.
7. The individual(s) who altered the names of the folders containing the alleged contraband photographs so that it appeared the dates provided in the file names corresponded to the EXIF data of files in those folders. We further request the true and original folder dates.
8. The individuals(s) who backdated the folder content and rolled back the system time to 2003 before manually copying these files onto the seized hard drive. This request is in relation to the fact that all the files in the Dell Dimension backup folder have a created date of July 26, 2003, despite the folder name indicating the backup date as March 30, 2009, the same date that appears on all the files' created dates.
9. All examination notes of the forensic examiners.
10. Photographs of the camera's CF card, documenting its condition and packaging, when received by FE Flatley on 02/22/2019 and by FE Booth on 06/10/2019.
11. All communications, including but not limited to texts, e-mail messages, notes, and voicemail messages, of FET Donnelly, FE Booth, FE Flatley, SA Lever, and SA Jeffrey, SA Mills, SA Weniger, AUSA Hajjar, AUSA Penza, AUSA Lesko, regarding this case.
12. The original forensic image (NYC023721_1B16.E01) and file listing of the WD HDD (1B16) created by FET Donnelly (NYC023721_1B16.E01.csv) and the imaging log for that item.

[1] Accordingly, any evidence related to manipulation, alteration, or chain of custody breaks with said evidence should have been disclosed by the government in advance of trial.

13. The FTK log of the processing, browsing, searching, and bookmarking of evidence for the WD HDD (1B16) and both instances of processing for the camera's CF card (1B15a).
14. The forensic image of the camera's CF card created by FE Flatley (NYC024299.001), together with its imaging log and file listing (.CSV) file.
15. The forensic image of the camera's CF card (1B15a) created by FE Booth (NYC024299_1B15a.E01), together with its imaging log and file listing (.CSV) file.
16. The CART Requests corresponding to SubID 196817 and SubID 208206.
17. All EXIF data for ALL photographs listed on both of the camera's CF card reports (GX 521A, dated 04/11/2019, and GX 521A Replacement, dated 06/11/2019).
18. The logical file layout of the camera's CF card

Witness Collusion and Tampering

1. All 3500 materials, including 302 notes, and all internal memoranda, including FBI messages, emails, and other communications regarding witnesses and witness meetings not previously provided;
2. All aforementioned materials specifically as they pertain to:
   a. India
   b. Siobahn Hotaling
   c. Michele Hatchette
   d. Danielle Roberts
   e. Samantha LeBaron
   3. All aforementioned materials specifically as they pertain to:
   a. Mark Vicente
   b. Souki
   c. Audrey
   d. Crystal
   e. Sarah Edmondson
   f. Nicole
   g. Daniela
   h. Catherine Oxenberg
   i. Jessica Joan ("Jaye")
4. All text messages and email communications between the individuals reference in 3) between May 2017 and May 2019;
5. All documentation or communications between FBI agents and/or AUSAs concerning FBI conduct that could be perceived as direct or indirect witness intimidation;
6. All emails, text messages, letters, or other forms of written communication between Neil Glazer and the government, including the United States Attorney's Office and FBI;
7. Any audio recordings of Neil Glazer;
8. Any audio recordings, text messages, or other forms of communication between witnesses prior to any testimony.

Nicole Travels

1. Any Amtrak, Greyhound, or other commercial train or bus receipts, with corresponding dates and times, provided to the FBI and/or Justice Department concerning Nicole's train or bus travels to Albany where the purported sex acts occurred.

2. Any payment information concerning Nicole's method of payment of the abovementioned travel.
3. Any other documentation concerning the dates, times, and modes of Nicole's travels.

Mr. Raniere's Arrest

1. Any text messages, phone calls, emails between individuals from the United States Justice Department, including but not limited to the FBI, DEA, and U.S. Attorney's Office, any private citizens, and/or diplomats to further the detention, arrest, or capture of Mr. Raniere.
2. Any information concerning the arrest of Mr. Raniere upon his arrival in the US, including the identification of the arresting agents, any information concerning the purchase of the commercial airplane ticket for Mr. Raniere from Mexico to Texas, after his capture in Mexico, and the passenger manifest for that flight.
3. Any information concerning the capture of Mr. Raniere in Mexico on March 25, 2018, including the identification of the individuals involved in the capture.
4. Any official records of deportation, extradition, or expulsion of Mr. Raniere from Mexico.

We expect that the requested materials be produced as soon as possible given their already untimely production. If the government needs clarification of any of the above requests, please do not hesitate to contact me.

Very truly yours,

Joseph Tully

EXHIBIT C

U.S. Department of Justice

United States Attorney
Eastern District of New York

TH
F. #2017R01840

271 Cadman Plaza East
Brooklyn, New York 11201

March 18, 2022

By Email

Joseph M. Tully, Esq.
Tully & Weiss
joseph@tully-weiss.com

Re: United States v. Keith Raniere
Criminal Docket No. 18-204 (S-2) (NGG)

Dear Counsel:

The government is in receipt of your letter dated March 16, 2022.

The government fully complied with its obligations pursuant to Rule 16 of the Federal Rules of Criminal Procedure, 18 U.S.C. § 3500, and Brady v. Maryland, 373 U.S. 83 (1963) and its progeny prior to the jury trial in this case.

Very truly yours,

BREON PEACE
United States Attorney

By: /s/
Tanya Hajjar
Assistant U.S. Attorney
(718) 254-7000

EXHIBIT D

Declaration of Dr. James Richard Kiper, Ph.D.

1. I served as an FBI Special Agent for 20 years, from 1999 to 2019.
2. In the FBI, I served as a case agent, a supervisor, a unit chief, a forensic examiner, a trainer of forensic examiners, and a trainer of other trainers of forensic examiners. I have an in-depth knowledge of FBI digital evidence examination procedures and policies.
3. I have previously signed the protective order related to reviewing discovery in this case. I have extensively reviewed discovery that I have been provided by Mr. Raniere's counsel and have written affidavits averring to unmistakable evidence of criminal tampering in Mr. Raniere's underlying criminal case as occurring on two pieces of evidence, a camera card (1B15a) and a western digital hard disc drive (1B16).
4. If I had access to four specific evidence items which are currently in the possession of the government but have never been provided to the defense, after forensic testing, I could make further determinations as to the camera card (1B15a) and the western digital hard disc drive (1B16) regarding when and how the illegal tampering took place. These four evidence items are 1.) a copy of the camera card dated April 11, 2019, NYC024299.001 and its corresponding FTK log file NYC024299.001.txt, 2.) a copy of the camera card dated June 11, 2019, NYC024299_1B15a.E01, and its corresponding FTK log file, NYC024299_1B15a.E01.txt 3.) the CSV file listing for the image of the WD hard disc drive taken on September 19, 2018 (NYC023721_1B16.E01.csv), and 4.) Examination notes taken by SFE Flatley during his April 11, 2019 forensic examination of the camera card, and the associated FTK log files.
5. The four requested items are narrowly tailored to guarantee to provide further exculpatory evidence since they will contain the same manipulated data that, even given my limited access to discovery, I have already demonstrated such to have been falsified.
6. Further testing of these four items could, given the circumstances of the crime and the evidence marshaled against Mr. Raniere at trial, establish to a certainty whether the metadata that was used in trial to establish the dates that the twenty-two alleged contraband photos were taken is authentic or is a result of fabrication.
7. I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct, and of my own personal knowledge, except as to those matters stated upon information and belief. As to those matters, I believe them to be true.

Executed on March 13, 2023

James Richard Kiper, Ph.D.

EXHIBIT E

Declaration of Stacy R. Eldridge, CFCE, GCFE, LPD

1. I served as a professional support employee of the Federal Bureau of Investigation (FBI) from 2003 to 2012.
2. In the FBI, I served as an Information Technology Specialist (ITS), a Forensic Examiner (FE) on the Computer Analysis Response Team (CART), and Senior Forensic Examiner (SFE) on CART, and a Digital Evidence Instructor for CART Headquarters.
3. In these roles I conducted over four hundred examinations on over 100 TBs of data, mentored and trained CART Forensic Examiners in Training (FETs), CART Techs, trained and graded Special Agents in the Digital Evidence Extraction Tech (DeXT) program, trained law enforcement personnel to use Image Scan, and trained and graded CART FETs on the Quality Manuals, Standard Operating Procedures, and evidence processing, and graded CART FE yearly proficiency tests. I have an in-depth knowledge of FBI digital evidence examination procedures and policies.
4. I have previously signed the protective order related to reviewing discovery in this case. I have extensively reviewed discovery that I have been provided by Mr. Raniere's counsel.
5. In my report, Summary of Technical Findings, dated September 29, 2022, I concluded that evidence tampering had occurred on a hard drive (1B16) and a camera card (1B15a) which the Government used, in this case, to prove certain RICO acts. I also concluded that the camera card data was altered while in the custody of SA Michael Lever.
6. If I had access to four specific evidence items which are currently in the possession of the government but have never been provided to the defense, after forensic analysis, I could make further determinations as to the camera card (1B15a) and the western digital hard disc drive (1B16) regarding when and how the illegal tampering took place. These four evidence items are 1.) a copy of the camera card dated April 11, 2019, NYC024299.001 and its corresponding FTK log file NYC024299.001.txt, 2.) a copy of the camera card dated June 11, 2019, NYC024299_1B15a.E01, and its corresponding FTK log file, NYC024299_1B15a.E01.txt 3.) the CSV file listing for the image of the WD hard disc drive taken on September 19, 2018 (NYC023721_1B16.E01.csv), and 4.) Examination notes taken by SFE Flatley during his April 11, 2019 forensic examination of the camera card, and the associated FTK log files.

7. The four requested items are narrowly tailored to guarantee to provide further exculpatory evidence since they will contain the same manipulated data that, even given my limited access to discovery, I have already demonstrated such to have been falsified.
8. Further testing of these four items could, given the circumstances of the crime and the evidence marshaled against Mr. Raniere at trial, establish to a certainty whether the metadata that was used in trial to establish the dates that the twenty-two alleged contraband photos were taken is authentic or is a result of fabrication.
9. I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct, and of my own personal knowledge, except as to those matters stated upon information and belief. As to those matters, I believe them to be true.

Executed on March 16, 2023

Stacy R. Eldridge

Stacy R. Eldridge, CFCE, GCFE, LPD